scientific reports

Check for updates

OPEN

Secure and flexible image watermarking using IWT, SVD, and chaos models for robustness and imperceptibility

Wafa Hamdan Alshoura & Moatsum Alawida✉

The utilization of Singular Value Decomposition (SVD) is widespread in several image watermarking methods to attain a more favorable balance between the demands of watermarking. Nevertheless, SVD exhibits some limitations, including false positives, limited capacity, and security issues. In order to overcome these challenges, a new approach to image watermarking has been introduced, which utilizes a combination of Integer Wavelet Transform (IWT), SVD, and chaos models. The generation of chaotic orbits in the scheme is based on utilizing chaotic variables generated through a secret key. The secret key is a major element in embedding, extraction, encryption, and ownership protection. The smooth generation of multiple scaling factors (MSF) matrices is achieved using chaotic points in the encryption stage. In order to attain a suitable equilibrium between watermarking robustness, imperceptibility, and security, the IWT technique is utilized to convert both the host and watermark images into frequency coefficients. The proposed method involves the extraction of a 4-bit matrix from the LL_1 sub-bands of the host image. This matrix is subsequently subjected to scrambling and merged with the watermark image, resulting in a 12-bit watermark image. Afterwards, the two sub-bands of the host image undergo two levels of IWT, and three sub-bands are chosen from the resultant 2-level image for embedding. The selected sub-bands are then subjected to SVD, where the embedding process utilizes the singular values S_i. The high-frequency sub-bands of the watermark image are embedded into the singular values S_i of the host image using chaotic MSF matrices. The scheme also encrypts the side information to achieve high security and protect the ownership. Even a slight change in the secret key can highly affect the proposed scheme, resulting in the generation of a noise image if an incorrect key is used. This feature makes the proposed scheme robust against false positive problem (FPP) attacks. Additionally, the proposed scheme can embed watermark images with high flexibility and low distortion, achieving high robustness and imperceptibility under different hybrid MSF matrices, outperforming several other schemes. With these features, the proposed scheme successfully fulfils the security and capacity requirements of a blind watermarking scheme, making it suitable for practical watermarking applications.

Keywords Watermark, SVD, IWT, Embedding, Chaotic map

Growing the advancement of digital applications and the rapid growth of network services, data protection is of particular concern at this time due to routine sharing and unauthorized activities such as copying, editing, altering, and integrity issues. Watermarking is one of the data protection technologies on top of other cybersecurity technologies such as cryptography and steganography[1]. Hiding methods (embedding and extraction process) are used in a digital watermarking scheme to provide copyright ownership production for the different data types. The embedding process conceals the watermark signals elsewhere in the cover (host) of digital data such as images, while the extraction process recovers the embedded watermark signals. And thereby, digital watermarking can be inserted into the embedding system for data secret. Digital watermarking can be used for several purposes to achieve many characteristics such as copyright ownership protection, authentication, tamper detection, and others[2–5].

Digital image watermarking can be classified into two main categories: visible and invisible watermarking. The visible watermarks do not need to embed watermark signals into a host image and only print logos or

Department of Computer Sciences, Abu Dhabi University, Abu Dhabi 59911, United Arab Emirates. ✉email: moatsum.alawida@adu.ac.ae

labels on the host image to keep ownership of the host image and to advertise easily to all. Adversaries can rapidly destroy and attack visible watermarks because they are easy to detect[6–9]. On the other side, the invisible watermark category embeds the watermark signals in the host image without being seen by the human visual system (HVS)[10,11]. The invisible watermark category is based on the idea of embedding watermark signals in unidentified sections of the host image. Three important requirements should be provided for the invisible watermarking scheme to be a practical scheme, these requirements are robustness, imperceptibility, and security. Robustness refers to the capability of a watermark to resist different attacks or modifications, ensuring that it cannot be easily removed or altered. On the other hand, imperceptibility pertains to maintaining the quality of the watermarked image after embedding, ensuring that it remains visually indistinguishable from the original. Security involves implementing measures to protect the watermarked image from unauthorized extraction attempts, preventing the unauthorized extraction of the original watermark or the insertion of counterfeit watermarks for false authorship claims.

A robust watermarking scheme ensures the visibility and recognition of the extracted watermark even under various attacks[12]. An imperceptible watermarking method aims to minimize the perceptible difference between the host and watermarked image, making it difficult to extract the embedded watermark or detect patterns resulting from the embedding process[13]. Evaluating the security of a digital image watermarking scheme requires its immunity to various attacks[2,12].

A watermarking scheme can be implemented in either the spatial or transform domain. In the spatial domain, the watermark is directly embedded into the host image by modifying the least significant bits (LSBs), resulting in minimal impact on pixel values and human visual system (HVS) perception. In the transform domain, the host image is first transformed into the frequency domain using methods like DCT, DFT, DWT, IWT, or SVD[14–16]. The watermark signals are then embedded by modifying the frequency coefficients, and the transformation process can be reversed. Transform-based methods offer better resistance against geometric and non-geometric attacks, but they have higher computational complexity compared to spatial-based methods[17].

Transform-based watermarking methods, such as combinations of different transformations, have been successful in achieving robustness and imperceptibility in image watermarking schemes[18–20]. However, these methods have limitations in terms of capacity, processing time, and security against specialized attacks. Increasing the capacity often leads to a decrease in the quality of the watermarked image, making it challenging to find the optimal trade-off. To overcome these limitations, the combination of SVD with other transformations has been employed in various schemes, including DWT+SVD[21], DWT+DCT[22], DCT+SVD[23], DWT+DCT+SVD[24], and IWT+SVD[25].

SVD is a mathematical tool and can be applied on the host image and watermark image, three matrices are generated (U, S, V^T). One of the three generated matrices of the host image is selected for embedding watermark signals. There are two general methods of SVD embedding in SVD-based image watermarking schemes. The first method is non-applied SVD on the watermark image, the watermark is directly embedded into the host image[26]. Where the host image is decomposed by SVD and one of the three matrices is selected for the embedding process. The second method is to apply SVD on the watermark image, the watermark is decomposed by SVD into three matrices ($U_W, S_W, {V_W}^T$), and one or two of them is used to embed into the host image[14,27,28]. Both methods decompose the host image after applied SVD transform into three matrices ($U_H, S_H, {V_H}^T$) and most of the existing SVD-based image watermarking schemes used singular values S to embed the watermark signals. Due to the accuracy of singular values S when faced with geometric and non-geometric (signal processing) attacks. Besides, the singular values Sdescribe the luminescence of the image with does not have geometric contents. However, two SVD methods suffer from FPPs and cannot face three FPP attacks[29].

FPP occurs in case embedding the watermark directly or S_W into S_H of the host image, FPP can be detected and extracted a fake watermark without knowing the original watermark[26,29,30]. One can use a fake reference image to extract a watermark. This scenario, therefore, performs an uncertainty case, and the issue of ownership cannot be tackled. One may claim another image from his/her fake reference image. The singular values of the host image S_H has luminescence, which means that has a very low impact on the geometric content. S_H consists of descending order non-negative values on the diagonal line of the matrix, and the remaining other values are zero. Once changing or removing or altering the diagonal S values, it will not more effect on the image after inverse SVD. Thus, an adversary can be extracted any values of S_H and will not impact the extracted fake watermark.

A lot of several solutions have been introduced to overcome FPP and enhanced SVD-based image watermarking schemes. These solutions are categorized into two groups: Embedding singular vectors and cryptographic techniques. In the first group, the singular vectors are left U and right V^T matrices of SVD transform, used one of them or principle component (left singular vectors and singular values) US_W in the embedding process[25,31,32]. Makbol et al proposed hybrid SVD-based image watermarking[25], they used a left singular vector matrix of watermark image U_W instead of S_W in the embedding process. The proposed scheme used multi-objective ant colony optimization (MOACO) to generate scale factor parameters to achieve a good trade-off between robustness and imperceptibility. The V_W and S_W of the decomposed watermark are used as side information to extract the original watermark in the extraction process. The FPP is removed and the proposed scheme successfully faces the FPP attacks. However, the robustness against geometrical and non-geometrical attacks is still weak.

Embedding principal component US_W group has been proposed in two schemes[31], US_W consists of U_w and S_W matrices and embeds into S_H of the host image. Whereas the ${V_w}^T$ is used as side information to extract the embedded watermark in the extraction process. ${V_w}^T$ has the geometrical content of the watermark image, without it, it is difficult to extract the embedded watermark. Thus, FPP is removed and the proposed schemes are straight and simple steps. However, U_W holds the geometrical content of the image, and small destruction

in its values leads to many distortions in the extracted watermark image. The proposed schemes are vulnerable to well-known attacks.

Cryptography algorithms provide an effective means to counteract FPP attacks in watermarking schemes. Specifically, the hashing, encryption, and digital signature techniques have been utilized in SVD watermarking images, as demonstrated by various studies[33–37]. In the hashing method, a one-way hash function is applied to the side information (U_W and V_W) to generate a hash value. The hash value is then stored after the embedding process is completed, while the side information is hashed again during extraction and compared with the stored hash value. The extraction process is permitted to continue when the two hashes match, while it is halted if they do not. On the other hand, the encryption process involves encrypting the watermark image before embedding it[35]. During extraction, decryption is carried out with the correct secret key to extract the watermark image. If the decryption process fails, a noise image is generated with no significance. These cryptographic methods have proven effective in eliminating the FPP issue, with the added advantage of integrating authentication procedures.

In[36,37], digital signature methods are introduced as similar to the prior methods, whereby, in the embedding process, the S_H of the host image is utilized. The proposed schemes focus on generating digital signatures from the side information to embed the watermark image into the host image. The extracted digital signature is used to authenticate with the stored digital signature. The digital signature methods have removed the FPP and demonstrated a good trade-off between watermarking requirements. However, these proposed methods that focused to remove FPP, have some drawbacks and limitations as follows:

1. Extra authentication processes are needed when extracting the embedded watermark image, which will increase computational overheads. That is because the authenticated data is embedded in the host image, which must be extracted for the matching process first. When the matching process is performed and the outcome is matched, then the extraction process can be completed. In addition, the hash values or digital signatures are embedded into the host images, any heavy cyber-attacks can destroy the embedded hash values or digital signatures[38,25].
2. Cryptographic techniques (hash value and digital signature) are very sensitive to a small change in input data and a key, which lead to some problems in the matching and authentication process. Some cryptographic attacks can destroy some of the parts of the embedded authenticated data, which leads to generating an un-authentication process[38,39].
3. The singular vectors used as side information in the extraction process, these have a lot of structural content of the digital image. Any changes or modifications resulting from the round-off mathematical operation in SVD transform lead to destroying the extracted watermark image. In addition, the side information is not secure from lost-information attacks or destroyed attacks[40,26].
4. A secret key is not considered in cryptographic technique solutions[41].The SVD-based watermarking scheme depends on the scaling factor αin the embedding and extraction process. A scaling factor uses to control the level of embedding and satisfy the proper balance between robustness and imperceptibility. There are two types of scaling factors; single scaling factor (SSF) and multiple scaling factors (MSF). An SSF is one value and multiplies all values in the matrix of the watermark image via dot product. A large SFF value leads to lower imperceptibility and resistance to attacks (high robustness), whereas a small SFF value leads to higher imperceptibility and weak under attacks. To cope with this issue, MSF is used instead of SFF, it consists of values sized in the embedded watermark matrix. To get optimal MSF values, optimization algorithms are used to find the optimal values by using popular algorithms such as genetic algorithms (GA)[42], particle swarm optimization (PSO)[43], multi-objective ant colony optimization (MOACO)[25]and differential evolution (DE)[23,41,44]. Even though optimal MSF algorithms have achieved a good trade-off between watermarking requirements, these algorithms need a lot of rounds to find the optimum MSF values and limited MSF range for each watermark.

SVD-based watermarking schemes encounter three main challenges: FPP attacks, limited capacity, and achieving a balance between watermark requirements and security considerations. FPP attacks can occur when utilizing singular values (S) during the embedding process. If an SVD-based scheme fails to defend against FPP attacks and allows the attacker to claim ownership of the host image, the scheme is considered insecure and fails to accomplish the primary objective of watermarking. The limited capacity of SVD-based schemes restricts the ability to add various watermark sizes to the host image. Conversely, increasing the size of the embedded watermark negatively impacts imperceptibility. Hence, achieving a balance between increased capacity and imperceptibility is crucial in this type of watermarking scheme. Furthermore, security measures are necessary to safeguard the watermarked image against unauthorized access or modifications. However, enhancing the security of the watermarking process may introduce complexity, potentially affecting the fulfillment of watermarking requirements (capacity, robustness, and imperceptibility). Striking a balance between the complex secure watermarking process and the desired watermarking objectives is another challenge that needs to be addressed in the proposed scheme.

Several existing IWT-SVD based watermarking schemes have laid the groundwork for new approaches. Arsalan et al.[45] introduced IRW-Med, a novel reversible watermarking technique designed specifically for protecting patient and medical information. This technique utilizes a companding function to minimize distortion during watermark embedding and leverages IWT for reversibility. Additionally, histogram processing is incorporated to prevent underflow/overflow issues. Notably, the intelligent selection of wavelet coefficients through Genetic Programming (GP) ensures an optimal trade-off between imperceptibility and watermark capacity.

Furthermore, Shi and Lv proposed a new blind watermark algorithm specifically designed for color images, aiming to enhance ownership protection and tampering detection[46]. This algorithm involves transforming the

original color image from RGB to the YUV color space, followed by applying the Arnold transform to construct the watermark. The secure image-adaptive watermark is subsequently embedded into the low-frequency coefficients of the original image through the modification of Discrete Integer Wavelet Transform (DIWT).

Makbol and Khoo introduced two watermarking schemes that address the False Positive Problem (FPP) through the combined application of IWT and SVD. The first scheme, presented in[26], embeds a watermark and generates a signature based on two singular vectors extracted from the embedded image. Notably, this signature is obtained prior to any processing of the watermark during the extraction phase. In contrast, the second scheme, described in[47], employs a multi-step approach. Following IWT applied to the host image, SVD is performed on all resulting sub-bands. To enhance security, an Arnold transform scrambles the watermark before its direct embedding into the singular values of the host image. IWT and SVD are efficient techniques for image watermarking. However, most approaches only apply IWT directly to the host image and embed the watermark image directly into the frequency values. Some existing methods have limited embedding capacity. Security relies on scrambling methods, such as the Arnold transform, and optimization algorithms are employed to achieve a balance between watermarking requirements.

In this paper, a new secure hybrid SVD-based image watermarking scheme is proposed to solve the above-mentioned challenges. IWT is used to transform the host and watermark images into frequency coefficients to achieve a balance between watermark requirements (robustness, imperceptibility, and security)[48]. A matrix of 4-bit of the LL_1 sub-bands of the host image is extracted and scrambled, and it is combined with the watermark image to generate a new watermark image with 12-bit. Two levels of the IWT are applied on the two sub-bands of the host image, and three sub-bands of the 2-level of the host image are selected to complete the embedding process. SVD is applied on the selected three sub-bands and the singular values S_i are used in the embedding process, the high-frequency sub-bands of the watermark image are embedded into the singular values S_i of the host image under the control of the chaotic MSF matrices. The inverse SVD with modified ${S_i}^{NEW}$ is applied and then the inverse (iIWT) transform is applied to obtain the watermarked image. The novelty of this proposed scheme is the embedding strategy, which is conducted on HH_1 and LL_1 sub-bands at the same time to fulfil the watermark requirements. Moreover, chaotic maps are used to encrypt the side information to increase the security of the scheme. A secret key is used to generate chaotic variables and it is stored in the certified authority (CA) and with the owner of the host image to ensure the secure scheme and overcome FPP attacks. The proposed scheme fulfills a balance between watermarking requirements (robustness, imperceptibility, and security), and the FPP is removed in different ways (secret key, combination process, and encryption side information). Capacity is also improved by different watermarks that can be embedded into other sub-bands in the second level IWT of the host image. The proposed scheme is secure and robust against various geometrical and non-geometrical attacks.

The primary contributions of the proposed image watermarking scheme are as follows:

- The scheme embeds the watermark image simultaneously into both the HH_1 and LL_1 sub-bands of the host image, enhancing robustness and imperceptibility.
- To counteract FPP attacks and preserve the integrity of the embedded watermark, a portion of the host image is incorporated into the watermarking process.
- A secret key is utilized to generate chaotic variables, which are securely stored by both the certified authority (CA) and the owner of the host image. This dual storage mechanism strengthens security and mitigates the risk of FPP attacks.The remainder of this paper is structured as follows: In Section 2, a brief overview of SVD, IWT, and chaotic maps is provided. The proposed scheme is then described in detail in Section 3, followed by the presentation of the experimental results in Section 4. This includes tests for imperceptibility and robustness, FPP analysis, evaluation of secret key sensitivity, as well as comparative analysis with other existing schemes in Section 5. The discussion is presented in Section 6. Finally, the paper is concluded in Section 7

Preliminaries

Singular Value Decomposition (SVD)

SVD is a mathematical analysis tool in linear algebra, which decomposes any matrix A into three matrices (singular values S and singular vectors (U and V)). It is used in different applications such as compression, image coding, and watermarking because it is simple and does no need computational operations. A digital image P is a matrix of 8-bit values $P \in \mathbb{R}^2$, it has a size of three dimensions, $1 \times M \times N$ for a gray image and $3 \times M \times N$ for a color image, where M and N are height (number of rows) and width (number of columns) of the matrix, respectively. SVD can be applied on P and three matrices are generated U, S, V^T, and these three matrices can be also regenerated to the original matrix P as follows

$$SVD(P) = U_P S_P V_P = \sum U_P * S_P * {V_P}^T, \tag{1}$$

where U_P and V_P are singular vectors, which are orthogonal matrices of $\mathbb{R}^2$, whereby S_P is a diagonal matrix of $\mathbb{R}^2$.

Figure 1 shows the three matrices of block 4×4 of a digital image. The left and right matrices are singular vectors, which are extremely sensitive to any altering in the U_P and V_P. S_P holds positive singular values in descending order $S_1 > S_2 > S_3 > \ldots > S_n$. The following SVD characteristics motivate the researchers to use SVD in the image watermarking schemes:

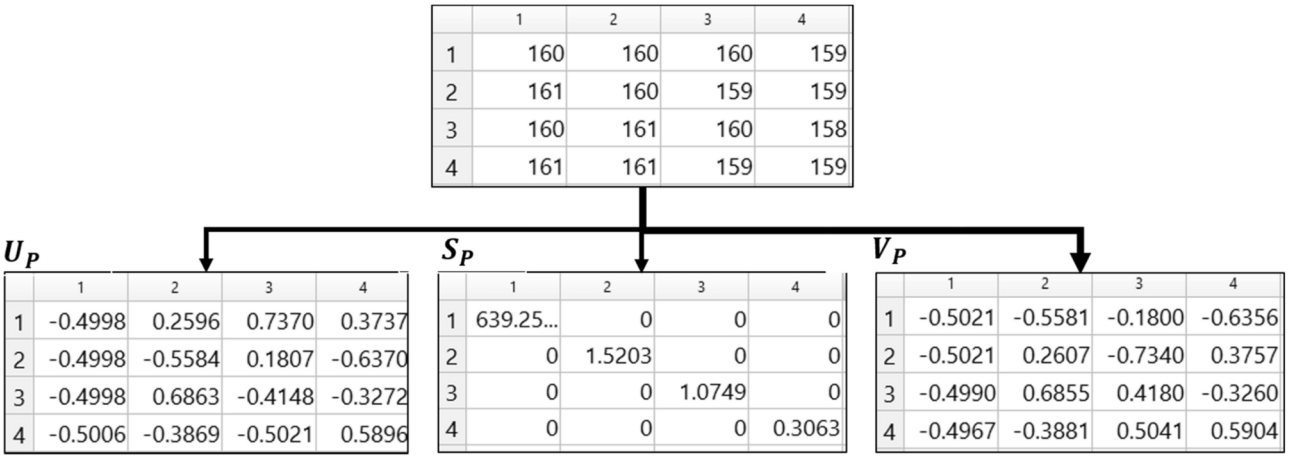

Fig. 1. Three components of the SVD of the matrix 4*times*4.

- Singular values *S* show high stability, and small changes to these values will not lead to a high impact on image pixels after inverting SVD. Thus, a watermarked image keeps a high imperceptibility with the host image.
- The image P' after inverting SVD, has the ability to resist the different well-known attacks.
- SVD is simple and does not need more computational operations.

Integer Wavelet Transform (IWT)

Lifting wavelet transform (LWT) is one of the frequency transformations and adapting wavelets to general settings. It is utilized in many applications such as signal processing, data compression, and watermarking. All classical transformation methods take input data and convert it to wavelet coefficients. And even if the input data is an integer number, the output is a floating number. It is essential to use one round-off operation to round to integer numbers in inverse transformation operations. Hence, classical methods lose information that is a perfect structure property. To cape this issue in digital image processing, the lifting system has a significant feature that converts the integer numbers into integer numbers without rounding propagation errors[49]. The integer-based lifting is called IWT.

IWT consists of three sub-processes, which are spilled, predict, and update, which is reversible without loss of information. It is faster than LWT and is more powerful. It has functionality that can be used to improve robustness and imperceptibility. Figure 2 shows two IWT levels of the Peppers image, where four sub-bands are generated. In the context of multi-resolution frequency sub-bands, there exist four non-overlapping sub-bands, namely LL (approximation sub-band), LH (horizontal sub-band), HL (vertical sub-band), and HH (diagonal sub-band). The finest scale wavelet coefficients are expressed by LH, HL, and HH, while LL expresses the coarse-level coefficients. It is noteworthy that LL plays a crucial role in the inverse IWT process utilized to reconstruct the original image after the IWT. Figure 3 shows the restored image with different cases to the sub-bands. In these cases, the image is restored by altering the sub-bands values such as ($iIWT(LL, LL, LL, LL)$). The LL sub-band has high impact than others and holds the geometrical structure of the image. Therefore, the LL sub-band is low imperceptibility compared to the rest sub-bands.

Chaotic map

A chaos model is a mathematical model and iterative function to generate chaotic points as trajectories in different dimensions. A chaos model is a nonlinear dynamic system and can be one-dimension (1D) and multi-dimensions (MD)[50]. Each chaos model consists of a mathematical iterative function, control parameter, initial state, and chaotic state. The chaotic maps have desired properties that are motivated for use in many application algorithms such as cryptography and watermarking[51]. These properties include unpredictability, maxing property, random-like behavior, and nonlinearity. Digital chaotic maps exhibit high sensitivity to slight variations in initial state and control parameters, which leads to producing a new totally chaotic trajectory. A 1D chaotic map is a simple mathematical system that not needs too many operations and can produce chaotic properties.

In this paper, we select two 1D chaotic maps to employ in the image watermarking scheme, these two maps are logistic-G and sine-G maps that were proposed to enhance the chaotic performance of classical logistic and sine maps[13,52]. The finding of two chaotic maps depicts a large chaotic parameter range and high chaotic complexity. These two maps can be defined as

$$x_{n+1} = (r_1^2 \times x_n \times (1 - r \times x_n) + \frac{r_1}{x_n}) \ mod \ 1 \tag{2}$$

$$y_{n+1} = (r_2 \times sin(\pi \times r_2 \times y_n) + \frac{r_2}{y_n}) \ mod \ 1 \tag{3}$$

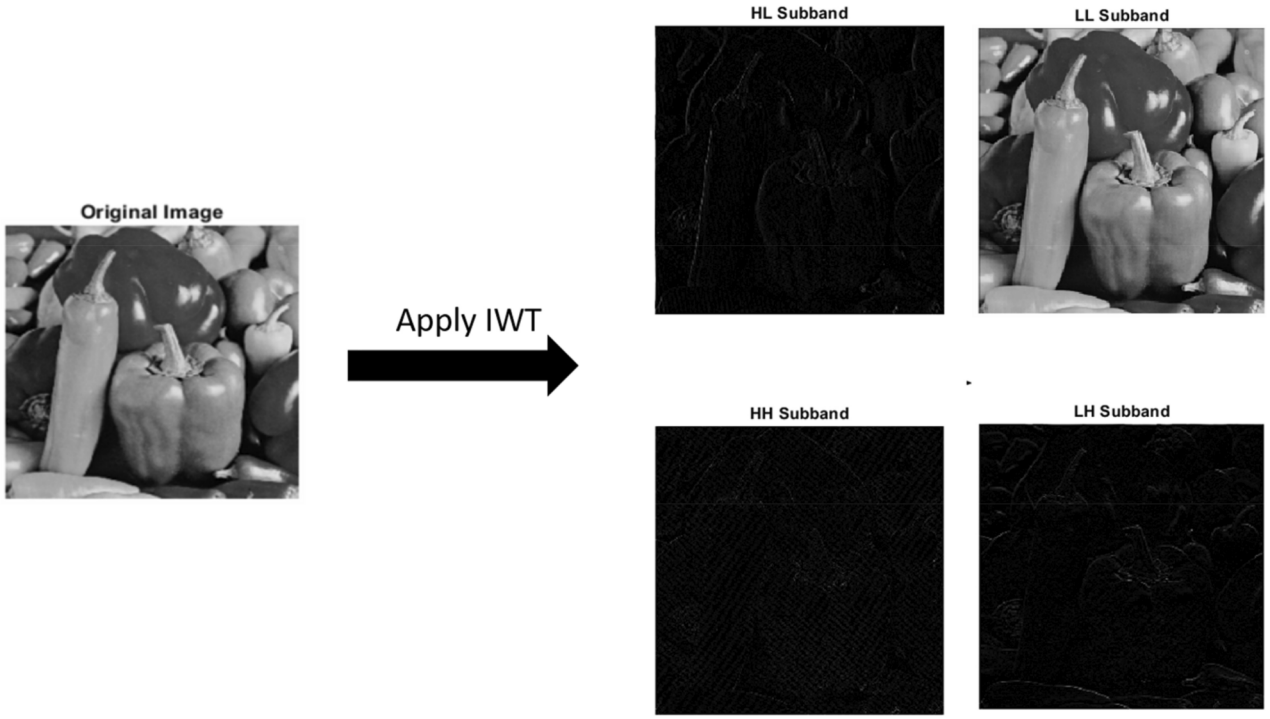

Fig. 2. IWT sub-bands of P, change to two levels.

where x_n and y_n are chaotic state within interval (0, 1), and r_1 and r_2 are control parameters within range $(0, \infty)$. We refer to the modified logistic and sine maps as logistic-G and sine-G respectively.

It is very important to show the chaotic performance for two maps, bifurcation diagrams and Lyapunov exponent (LE) are used in this analysis. Bifurcation diagrams show the chaotic regions to the control parameters, Figures 4 and 5 depict the relationship between chaotic states with control parameters, we can see the shaded regions more than unshaded regions, shaded regions mean that the chaotic behaviors can be generated at this control parameter with range (0,1). Furthermore, when unshaded regions are generated, which means that the chaotic state is in a fixed point or limited cycle. Thus, the two maps are chaotic and large chaotic parameters. LE is a mathematical tool to measure the sensitivity to the initial state under different parameter settings. The LE has large positive values which means the chaotic map is high sensitivity and the chaotic states divergence quickly as time pass. Whereas the negative or zero LE values that implies non-chaotic behaviors. In Figure 6, large LE values over control parameters can be shown, and it can be observed that the two maps have chaotic behaviors and high sensitivity. Based on these indicators, we have selected the enhanced logistic and sine maps in the proposed watermarking scheme.

Proposed scheme

To achieve high robustness and imperceptibility, the MSF parameters are generated via AI search optimization algorithms to obtain optimal values, balancing watermarking requirements. In this scheme, a chaos-based MSF approach generates multiple MSF matrices. Two chaotic maps are iterated to produce highly random chaotic states. These trajectories are used to generate a random matrix, and the side information is encrypted using the chaotic states to enhance security and protect ownership rights. This strategy offers low computational overhead, security, and flexibility.

Our watermarking scheme leverages the strengths of both the IWT and SVD. The IWT is first applied to the image, and specific bands are selected for watermark embedding. SVD is then applied to these selected bands, providing the high embedding capacity necessary for substantial watermark data. This combined approach capitalizes on the lossless nature of the IWT, ensuring perfect image reconstruction before watermarking, and the large capacity offered by SVD, resulting in a scheme that balances embedding capacity with efficient performance.

The IWT and SVD possess characteristics that contribute to achieving high watermarking requirements. The IWT provides superior spatial-frequency localization[53], dividing an image into four bands: low-low (LL), high-low (HL), low-high (LH), and high-high (HH). In our scheme, the IWT is applied twice to the host image and once to the watermark image. The IWT coefficients of the host image are then subjected to SVD, and three high-frequency sub-bands of the watermark image are embedded within the singular values of the host image. MSF parameters can be generated at various scales, allowing for desired requirements to be met at each scale.

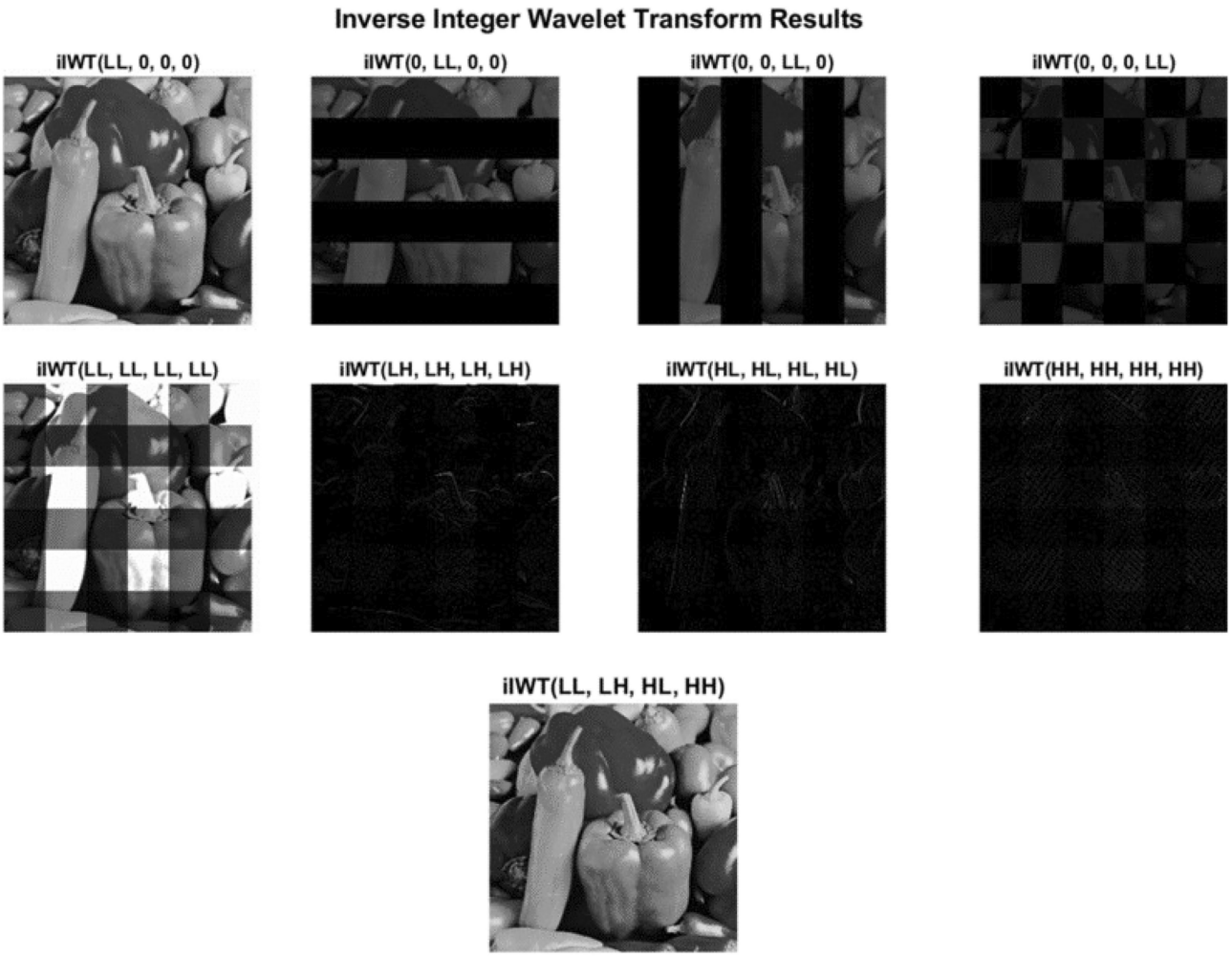

Fig. 3. Different cases for inverse IWT.

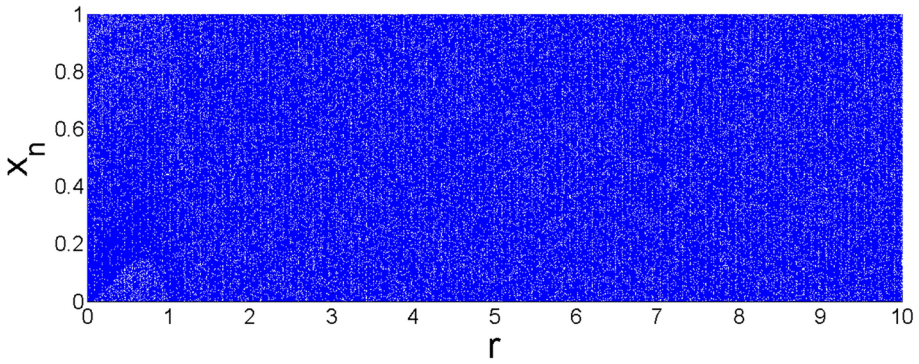

Fig. 4. Bifurcation diagram of the logistic-G chaotic map.

A secret key plays a crucial role in securing the proposed scheme, providing secure and flexible control. This key is used to generate the initial conditions and control parameters of the chaotic maps. The resulting chaotic points are used in the scrambling method, encryption algorithm, and matching process. The host image is decomposed by the IWT into four sub-bands, and the LL sub-band is used to recombine with the watermark image, creating a new matrix.

The proposed watermarking scheme comprises four phases: MSF generation, embedding, extraction, and encryption. The MSF generation phase uses chaotic maps to generate MSF parameters within a suitable range for the embedding phase. The chaotic maps are iterated to produce random values used in the embedding and

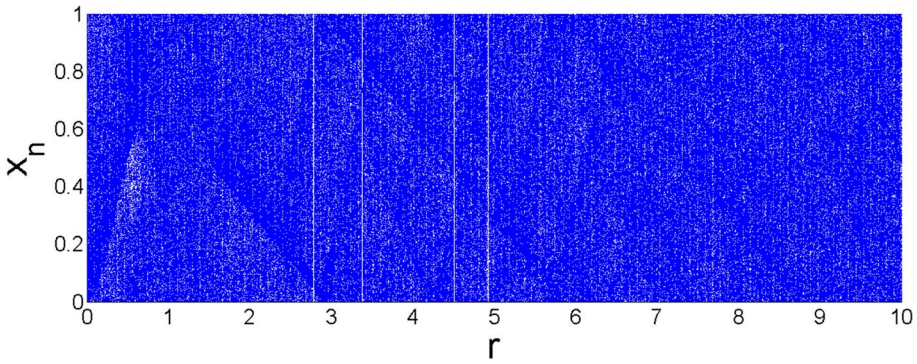

Fig. 5. Bifurcation diagram of the sine-G chaotic map.

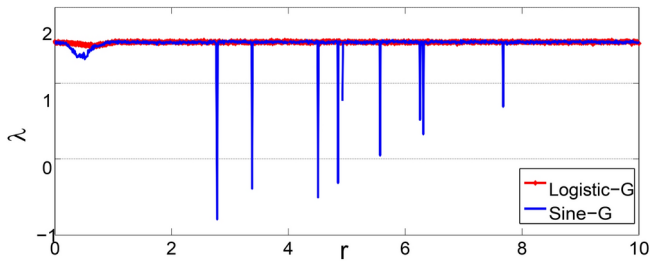

Fig. 6. Lyapunov exponent of the two enhanced chaotic maps.

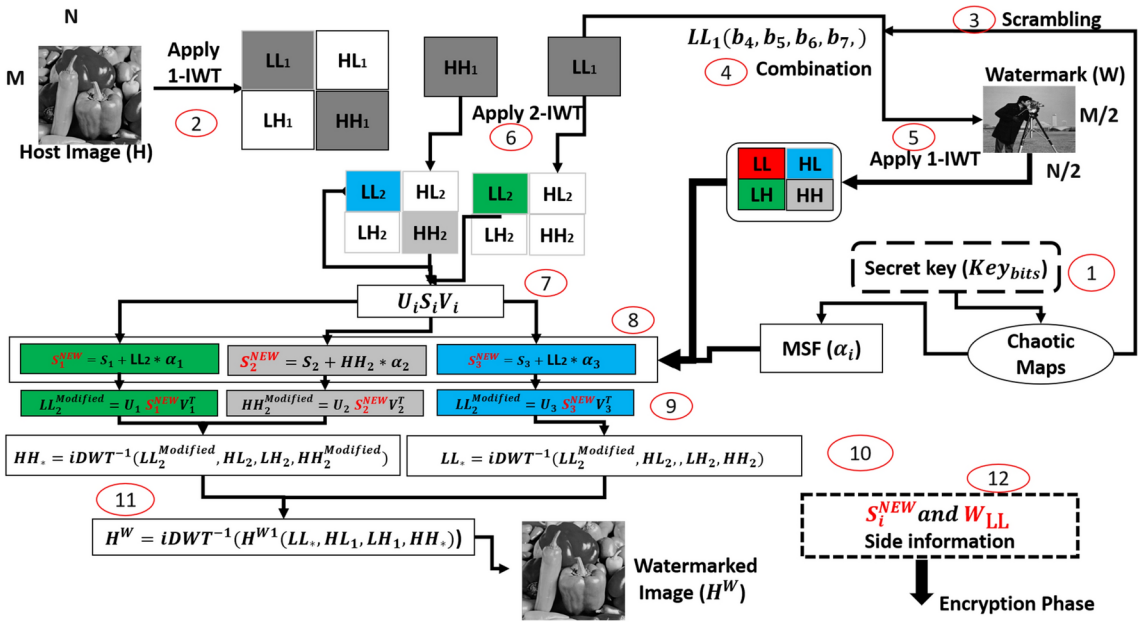

Fig. 7. The embedding process of the proposed scheme.

extraction phases. The encryption phase is performed based on the generated chaotic points. Further details of the embedding and extraction phases are illustrated in Figures 7 and 8, respectively. These four phases are discussed in detail in the following subsections.

MSF generation

Digital chaos is a mathematical model and can produce randomness and unpredictability digital points, the chaotic points can be generated by iterated chaotic maps to $M \times N$ times, where M and N are numbers of rows and columns in the watermark image. Firstly, we used the enhanced classical 1D chaotic maps to overcome a set

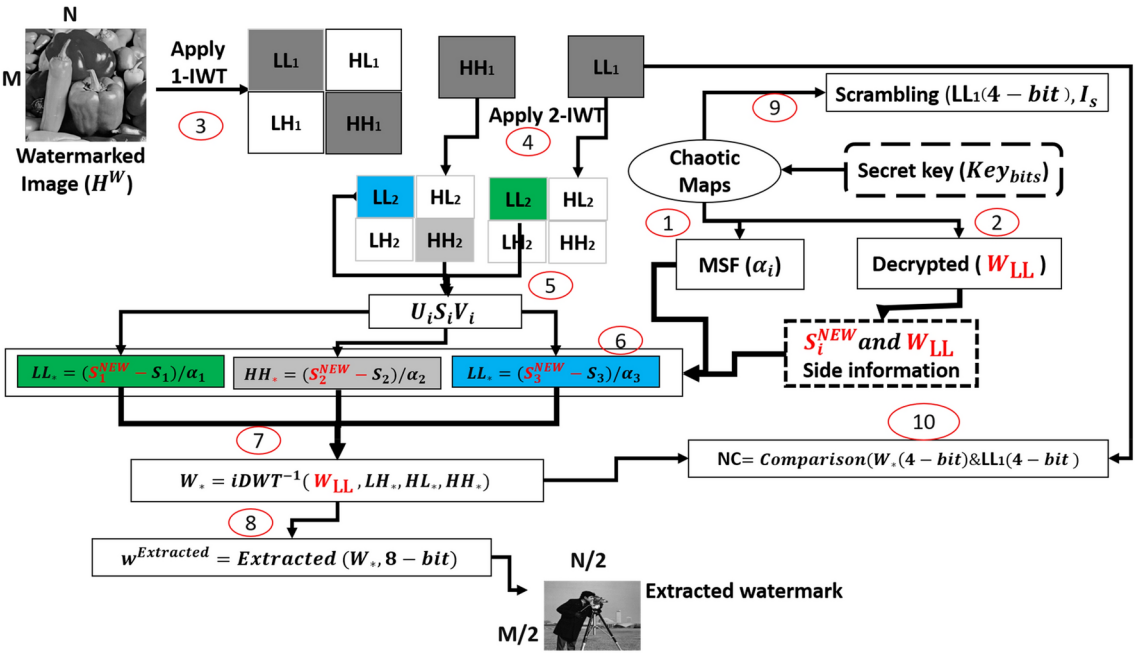

Fig. 8. The extraction process of the proposed scheme.

of security issues found in classical maps such as limited keyspace and low complexity. Two enhanced chaotic maps are used to generate a new matrix A. Two control parameters and two initial values are derived from a secret key K for the proposed watermarking scheme. Based on the cryptography rules, a secret key should be at least 128-bit to be extremely difficult to predict by brute force attack and it should be quite sensitive to a tiny change. Therefore, 128-bit of the random bit stream is considered a secret key and it is used to generate the control parameters and the initial values for chaotic maps. The following steps show the way in which the control parameters and the initial value are derived from a secret key K.

Step 1. The mean value M_K of the K is calculated and multiplied by 0.9^7 to increase the sensitivity of the secret key.

Step 2. The control parameters (r_1 and r_2) and initial values (x_0 and y_0) are calculated as below:

$$x_0 = \sum_{i=1}^{52} \frac{k(i) + M_K}{2^i}, \tag{4}$$

$$y_0 = (\sum_{i=53}^{104} \frac{k(i) + M_K}{2^{i-52}} + x_0)\ mod\ 1, \tag{5}$$

$$r_1 = (\sum_{i=1}^{8} k(i) \times 2^i + \sum_{i=25}^{76} \frac{k(i)}{2^{i-24}} + y_0)\ mod\ 10 + 10, \tag{6}$$

$$r_2 = (\sum_{i=121}^{128} k(i) \times 2^{129-i} + \sum_{i=77}^{128} \frac{k(i)}{2^{i-76}} r_1)\ mod\ 10 + 10, \tag{7}$$

$$x_0 = (x_0 + r_2)\ mod\ 1. \tag{8}$$

Step 3.For the enhanced logistic and sine maps, the initial values are x_0, r_1 and y_0, r_2, respectively. The maps are iterated $M \times N$ times, storing the chaotic points in the matrices X and Y. The matrices X and Y should have the same size as the extracted singular values of the host image and the sub-band sizes of the watermark image. A final chaotic matrix A is then calculated based on these intermediary matrices as follows

$$A = \sum_{i=1}^{M} \sum_{j=1}^{N} \left(((x(i,j) + y(i,j) + M_K) \ mod \ C \right), \tag{9}$$

where $x(i, j)$ and $y(i, j)$ represent elements of the X and Y matrices, respectively, and i and j represent the row and column of A. The scale parameter C is used to determine the scale of MSF parameters. To achieve better trade-offs, C can be a small or large factor.

The consequent A matrix consists of random values within a state range of [0, C). Any changes to the secret key K would result in a completely different matrix due to the chaotic sensitivity of the enhanced chaotic maps and the mean value used in the A generated matrix. The secret key should therefore be maintained a protected with the owner's watermark image and CA.

Watermark embedding

In this phase, an image watermark is embedded into the host image by hybrid transforms. A grayscale image and color image can be used in this scheme and can be embedded in three host channels of the color host image. To be more clear and easy to explain, the grayscale image is selected in this scheme. The steps of the proposed embedding phase are as follows:

1. The host image H is transformed by using IWT into four sub-bands (LL_1, LH_1, HL_1,and HH_1).
2. The new matrix A that is generated of chaotic maps is sorted ascending and the new index of values I_s is generated and used to select the pixel values from LL_1 in the host image. A new scrambled matrix ${LL_1}^I$ is obtained that is generated by I_s to make a watermark secure and unreadable under different attacks. Figure 9 shows a numerical example of the scrambling process.
3. The generated sub-band ${LL_1}^I$ and the watermark W are converted to bit streams as (${LL_1}^I{}_B$ and W_B). The 4-bit stream for each value in ${LL_1}^I{}_B$ and corresponding pixel of the watermark W_B are recombined as $W(i,j)_{b0,b1,\ldots,b7}$ and $LL_{Ib0,b1,b2,b3}$. We select 4-bit of ${LL_1}^I{}_B$ to avoid combining 8-bit of the host image to the watermark and to reduce the computational overheads. The new matrix W' is used to complete the embedding process.
4. The W' is scrambled by using I_s of random matrix A to be more secure. W' has some information for the host image, which helps to protect the original watermark against different distortions. That is because most distortions impact on the least significant bits (LSB) of the watermark image, the LSB of the W' is extracted from LL_1, hence any distortions will effect the LSB and the original pixels of the watermark stay safe as possible as. Another reason to use LL_1 in the embedding is helped to overcome the FPP attack (second and third attacks) after completing the extraction process. The extracted $LL_{b0,b1,b2,b4}$ (after re-scrambled bits and removing them) compares with LL_1 of the watermarked image to check the owner rights (more details in watermarking extraction section).
5. The watermark image W' is transformed by IWT to generate four sub-bands (${W'}_{LL}$, ${W'}_{LH}$,${W'}_{HL}$, and ${W'}_{HH}$). Three high-frequency are used in the embedding process and the lower resolution approximation sub-band (${W'}_{LL}$) is used as side information because it has a rough description of the image and to protects it against different distortions. In case the embedding ${W'}_{LL}$, has two negatives impact on the host image and extracted watermark, it leads to low imperceptibility because of increasing the difference between the host and watermarked images. When it is susceptible to many distortions, it has a big impact on the extracted watermark image compared to other sub-bands. Three sub-bands of watermark are converted to fraction numbers by dividing 2^{12}, because the number of the bits is 12 (8+4), as follows

$${W'}_{LH} = \frac{{W'}_{LH}}{2^{12}} \tag{10}$$

$${W'}_{HL} = \frac{{W'}_{HL}}{2^{12}} \tag{11}$$

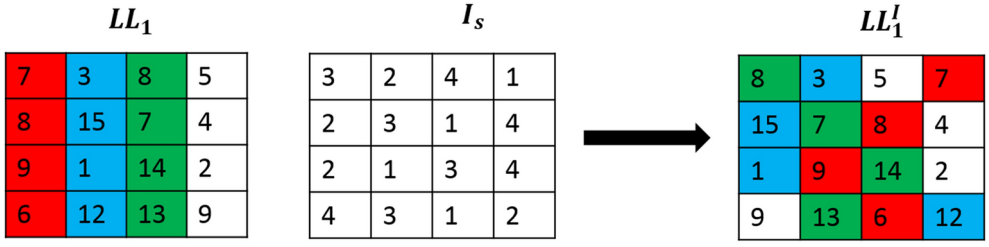

Fig. 9. The numerical example of the scrambling process for 4×4 matrix.

$$W'_{HH} = \frac{W'_{HH}}{2^{12}} \tag{12}$$

6. The LL_1 and HH_1 of the host image are selected and transformed by second-level IWT, whereby ${LL_2}^{LL_1}$, ${LL_2}^{HH_1}$ and ${HH_2}^{HH_1}$ of the host image are selected. Three sub-bands of W' are used in the embedding process (W'_{LH}, W'_{HL} and W'_{HH}). These sub-bands of the host and watermark images are carefully selected due to achieve a trade-off between imperceptibility and robustness, where *HH* achieves high imperceptibility and *LL* achieves high robustness against attacks. We embed three higher frequencies of the sub-bands of the watermark W' into three second-level sub-bands of the host image as below.

$$W'_{LH} \Rightarrow {LL_2}^{LL_1} \tag{13}$$

$$W'_{HL} \Rightarrow {HH_2}^{HH_1} \tag{14}$$

$$W'_{HH} \Rightarrow {LL_2}^{HH_1} \tag{15}$$

7. SVD is applied on three sub-bands (${LL_2}^{LL_1}$,${HH_2}^{HH_1}$), and ${LL_2}^{HH_1}$, to generate three matrices $U_i S_i V_i$ for each one. The singular values S_i are selected to complete the embedding process.

$$SVD({LL_2}^{LL_1}) = U_1 * S_1 * {V_1}^T \tag{16}$$

$$SVD({HH_2}^{HH_1}) = U_2 * S_2 * {V_2}^T \tag{17}$$

$$SVD({LL_2}^{HH_1}) = U_3 * S_3 * {V_3}^T \tag{18}$$

8. MSF parameters α_i are generated via the enhanced chaotic maps and factor C_i is controlled on the scale to achieve a trade-off between imperceptibility and robustness. We generate three MSFs for each sub-band.
9. The values of the three higher frequencies (horizontal (HL), vertical (LH), and diagonal (HH)) of the new watermark matrix W' are embedded into the singular values of the host image. The operation can be mathematically defined as

$${S_1}^{new} = S_1 + (W'_{LH}) \cdot \alpha_1 \tag{19}$$

$${S_2}^{new} = S_2 + (W'_{HH}) \cdot \alpha_2 \tag{20}$$

$${S_3}^{new} = S_3 + (W'_{HL}) \cdot \alpha_3 \tag{21}$$

where is the dot product operation. α_i is hybrid MSFs, we change the factor C_i values and obtain a new matrix with size equal to S_i size.

10. The modified ${LL_2}^{LL_1}$, ${HH_2}^{HH_1}$, and ${LL_2}^{HH_1}$ sub-bands are obtained by inverse iSVD as follows;

$${LL_2}^{LL_1 modified} = U_1 * {S_1}^{new} * {V_1}^T \tag{22}$$

$${HH_2}^{HH_1 modified} = U_2 * {S_2}^{new} * {V_2}^T \tag{23}$$

$${LL_2}^{HH_1 modified} = U_3 * {S_3}^{new} * {V_3}^T \tag{24}$$

11. The inverse IWT is applied by three modified higher frequency ${LL_2}^{LL_1 modified}$, ${HH_2}^{HH_1 modified}$ and ${LL_2}^{HH_1 modified}$, and the remaining detail sub-bands to obtain the one-level IWT coefficients, the inverse IWT second time is applied to obtain the watermarked image H^W. The ${S_i}^{new}$ and W'_{LL} are used as the side information for extracting process, where α_i can be generated by chaos models. The secret key is kept with the owner of the host image and CA, without the secret key, it is hard to obtain the extracted original watermark.

Encryption phase

Most of the image watermarking schemes used side information as the key[29]. However, it does not have the characteristic of the secret key such as sensitivity to small changes, and it has significant information for the embedded watermark. Figure 10 shows the new watermark image is generated by side information, the difference between the extracted watermark image and the original watermark image is low, which means an attacker can guess the watermark image if he/she has the side information without knowing the secret key. Hence, the side information should be protected and encrypted. Most of the schemes used third-party databases to keep the side information, it is a solution. The third-party database should be stored a small amount of data

Fig. 10. The watermark image generated by the side information.

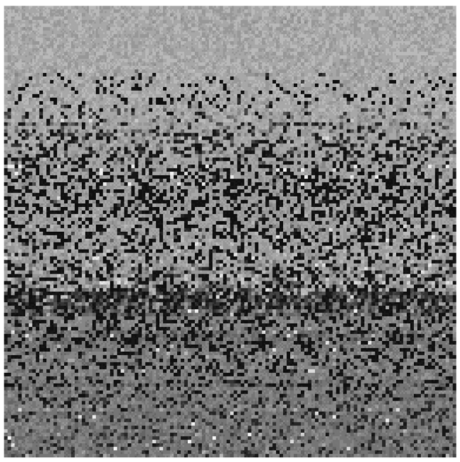

Fig. 11. The extracted watermark image with encrypted W'_{LL}.

for the watermarked image such as hash value or secret key. To make the algorithm flexible and secure, the side information should be encrypted.

In this phase, we encrypt the side information by the secret key and scrambling algorithm. S_i^{new} has some information such as the higher frequency of the sub-bands of the embedded watermark image, chaotic points, and singular values of the host image. If an attacker uses any singular values and he/she can generate three frequency sub-bands of the watermark image with only high-frequency coefficients. Thus, it is no need to encrypt or keep secure the S_i^{new} values. In contrast, W'_{LL} has significant information to the watermark image, hence it should be secured. Thus, W'_{LL} is encrypted by the index of matrix I_s, it has $M \times N$ integer numbers, we use I_s with size $\frac{M \times N}{2}$ to scramble W'_{LL}. Figure 11 shows the extracted watermark with scrambled W'_{LL} , we can see that the extracted image is random-like noise and unreadable. Figure 9 shows a numerical example of the scramble-based chaotic maps. The secret key is 2^{128} bits which are secure and hard to predict it by brute force attack.

The scrambling process depends on the secret key and enhanced chaotic maps. Scrambling operations are used to achieve a cipher image with confusion only. A scramble is a process to change the value positions randomly, which can achieve the confusion property. Here, we encrypt W'_{LL} by scrambling the positions of matrix values as follow:

1. W'_{LL} and A are transformed into one dimension array with size $\frac{M \times N}{2}$ for each one.
2. A is ascending sorted to be suitable for W'_{LL} size and I_s is generated.

3. The scrambling algorithm is conducted as follows:

$$[A, I] = x_1, x_2, ..., x_{\frac{M \times N}{2}} \tag{25}$$

$$A_{Sorted}, I_s = x_1(50), x_2(30), ..., x_{\frac{M \times N}{4}}(3) \tag{26}$$

$$W'^{Scrambled}_{LL} = W'_{LL}(I_s) \tag{27}$$

$W'^{Scrambled}_{LL}$ is a new scrambled matrix of the side information LL sub-band and it is hard to regenerate the same side information without the secret key. In this encryption phase, we just focus on the scrambling process and do not use a linear diffusion process such as Xor-operation, because the side information value has negative values, which needs more computation overheads to achieve the diffusion property.

Watermark extraction

In this phase, an owner would extract the embedded watermark from the watermarked image. There are some distortions and distorted parts in the watermarked image, which lead to difficulty in extracting the embedded watermark image. The distorted watermarked image resulted from geometric and non-geometric attacks. To extract the watermark image from the watermarked image, the secret key is used to decrypt the side information and to generate MSF parameters before starting this phase. The extraction steps are as follows:

1. Apply one-level of IWT on the watermarked image H^W, to obtain four sub-bands.
2. Apply second-level of IWT on the LL_1 and HH_2 to obtain four sub-bands for each one, ${LL_2}^{LL_1}$,${HH_2}^{HH_1}$, and ${LL_2}^{HH_1}$ are selected.
3. Decompose ${LL_2}^{LL_1}$,${HH_2}^{HH_1}$, and ${LL_2}^{HH_1}$ by SVD to obtain three matrix values for each one as

$$SVD({LL_2}^{LL_1}) = U_1 * S_1 * V_1 \tag{28}$$

$$SVD({HH_2}^{HH_1}) = U_2 * S_2 * V_2 \tag{29}$$

$$SVD({LL_2}^{HH_1}) = U_3 * S_3 * V_3 \tag{30}$$

4. The secret key is used to generate matrix A and generate the index I_s. $W'^{Scrambled}_{LL}$ is decrypted by I_s with size $\frac{M \times N}{2}$ to generate W''_{LL}. ${S_i}^{new}$ are three matrices of side information of the watermarked image, three MSF matrices α_i are generated by chaotic maps, and C_j.
5. Three higher frequency of the watermark image W''_{LH}, W''_{HL}, and W''_{HH} are extracted by computing as follow

$$W''_{LH} = ({S_1}^{new} - S_1) \cdot / \alpha_1 \tag{31}$$

$$W''_{HL} = ({S_2}^{new} - S_2) \cdot / \alpha_2 \tag{32}$$

$$W''_{HH} = ({S_3}^{new} - S_3) \cdot / \alpha_3 \tag{33}$$

where α_i is computed based on the chaotic maps.

6. W''_{LH}, W''_{HL}, and W''_{HH} are multiplied 2^{12} to obtain the integer numbers.
7. W''_{LL} and the extracted high frequency sub-bands W''_{LH}, W''_{HL}, and W''_{HH} are used to generate the new matrix W'' by inverse IWT as follows,

$$W'' = iIWT(W''_{LL}, W''_{LH}, W''_{HL}, W''_{HH}) \tag{34}$$

8. The generated matrix W'' has 12-bit in their values, the LSBs of 4-bit are extracted to be a new matrix ${LL_1}^I$, and the remaining 8-bit for each value is an extracted watermark $W^{Extracted}$.
9. The 4-bit that extracted ${LL_1}^I(b_0, b_1, b_2, b_3)$ from the watermark image is unscrambled by I_s.
10. The 4-bit that extracted ${LL_1}^I(b_0, b_1, b_2, b_3)$ from the watermark image and the 4-bit of the LL_1 watermarked image $LL_1(b_0, b_1, b_2, b_3)$ are compared to see the ratio of similarity. If the similarity is more than 50%, that means that the extraction process is accepted and the extracted watermark is correct. This method is subjected to the secret key power, due to the scrambling process conducted by chaotic maps.

Key management

Most image watermarking schemes keep the secret key with a third party known as a certified authority (CA)[19,54–57]. In this scheme, we keep the secret key with the owner and CA, because the owner is responsible for

the embedded watermark. Therefore, the side information is encrypted by the secret key to make the proposed scheme more protected. Anyone can claim his/her ownership of the digital image, and he/she can extract any watermark from the version of the digital image. Thus, the third party is more important to control the copyright protection of the digital image. The secret key is any random or meaningful binary value whose length is 128-bit, it should be kept with the version of the host image in the database of CA to ensure security and protection.

Generally, an owner has a host image, he/she embeds the watermark image or logo, then a watermarked image is distributed on the World Wide Web. An attacker can embed a watermark in the watermarked image by a different algorithm and different watermark images. An attacker will claim the ownership of the copyright of the digital image. Therefore, CA is a significant database to store digital images with their values to prove ownership and copyright. CA can protect digital images against attackers and their cyber-attacks claiming ownership of the digital images.

Experimental results and analysis

All experiments in this section are performed on five grayscale host images of size 512×512 (Airplane, Peppers, Baboon, Couple, and Boat), while the watermark image is Cameraman of size 256×256. We carefully selected five representative images from the SC-SIPI 'Miscellaneous' dataset[58]. These images cover a variety of categories, including trucks, airplanes, tanks, cars APCs, and even a male figure and an airport. Figure 12 depicts all of these images. All of the following experiments and the proposed scheme were implemented in MATLAB R2012b on a 64-bit processor with 6 GB RAM. All of the experiments and host images are given the same secret key. The images are divided into four sub-bands using the IWT 'Haar' wavelet. It can improve image resolution without causing rounding errors. The host image is divided into four sub-bands, and the *LL* and *HH* are chosen for embedding. To generate MSF parameters, secure side information, and achieve an acceptable balance between imperceptibility and robustness, chaotic points are used.

To ensure a comprehensive comparison with state-of-the-art methods, we conducted an in-depth literature review. Recognizing the varying levels of detail provided in existing research, we employed multiple tables to facilitate a fair and comprehensive comparison. This approach allowed us to effectively cover the key characteristics and performance metrics of different methods while considering the diverse information available in the literature.

Fig. 12. Host images (**a**) Peppers, (**b**) Baboon, (**c**) Couple, (**d**) Boat, (**e**) Truck, (**f**) Airplane, (**g**) Tank, (**h**) Car and APCs, (**i**) Male, (**j**) Airport, (**k**) the watermark image, Cameraman.

Imperceptibility and robustness analysis

Peak-signal-to-noise ratio (PSNR) and normalized correlation (NC) are two metrics that are consistently used in image watermarking schemes to assess imperceptibility and robustness. To determine the degree of similarity between two images, PSNR calculates the difference between the host image and the watermarked image. In an excellent watermarking scheme, a high PSNR value must be achieved which shows that the differences are barely discernible. PSNR is described as

$$PSNR = 10\log_{10}\left[\frac{max(H(i,j))^2}{MSE}\right] \tag{35}$$

where $max(H(i, j))$ is the largest pixel value in the host image, while the mean square error (MSE) between the host image H and the watermarked image H^W can be calculated as

$$MSE = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}[H(i,j) - H^W(i,j)]^2 \tag{36}$$

where M and N are the number of rows and columns of an image.

On the other hand, NC is continuously used and is calculated as W to determine the difference between an extracted watermark $W^{Extracted}$ and the original watermark W. NC is determined as

$$NC(W, W^{new}) = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[W(i,j) - \mu_1][W^{new}(i,j) - \mu_2]}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}[W(i,j) - \mu_1]^2}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}[W^{new}(i,j) - \mu_2]^2}} \tag{37}$$

where mu_1 and mu_2 represent, respectively, the mean values of W and W^{new}. When the extracted watermark image and the original image closely match one another, $NC \approx 1$. The original and extracted watermarks are identical when $NC = 1$.

Table 1 shows the PSNR scores for various MSF intervals to the five host images. Three MSF intervals are generated based on chaotic maps and scaling parameters C_i. In this proposed scheme, MSFs have the approximately same effect on the PSNR results and the five images have high PSNR values. Three matrices for each sub-band of the watermark image, these matrices values are under range (0,C_i). The imperceptibility between watermarked image and the host image on various MSFs and host images is high, which means that no more distortions in the watermarked image. An attacker cannot find any patterns between watermarked image and the host image by using visual or digital inspections. In addition, other proposed schemes have small SSF values that can achieve high PSNR values but are shockingly weak against geometrical and non-geometrical assaults. This issue can be solved by the proposed scheme, which uses three MSF parameters to enable both small and large MSF parameters to achieve high PSNRs. Next, small and large MSF parameters have no effect on robustness. In this scheme, the embedding strategy controls the findings of the scheme rather than seeking the best MSF parameters to achieve a successful trade-off between imperceptibility and robustness. *HH* and *LL* have value factors that enable successful trade-offs such as *LL* being resilient against attacks and *HH* keeping high-quality digital images after the embedding process.

Table 2 shows the NC scores of the proposed scheme using three MSF matrices. Regardless of whether the MSFs parameters are small or large, the proposed scheme can effectively extract the watermark, with NC

	MSFs (α_1, α_2, α_3)				
Test image	**(10,5,1)**	**(5,10,1)**	**(1,10,5)**	**(1,1,1)**	**(5,5,5)**
Peppers	43.82	43.75	43.70	43.84	43.91
Baboon	37.37	37.38	37.35	37.36	37.36
Couple	43.98	44.00	44.00	44.01	44.00
Boat	43.25	44.42	43.43	44.40	43.43
Truck	45.17	45.24	43.22	42.44	44.78
Airplane	43.70	43.58	43.78	44.40	43.98
Tank	39.94	40.88	41.24	41.40	41.43
Car and APCs	47.74	47.23	47.83	47.40	46.43
Male	46.17	49.14	48.43	48.40	47.41
Airport	41.15	42.32	43.53	45.70	41.13

Table 1. Imperceptibility (PSNR) results for different chaotic MSF values.

Test image	MSFs ($\alpha_1, \alpha_2, \alpha_3$)				
	(10,5,1)	(5,10,1)	(1,10,5)	(1,1,1)	(5,5,5)
Peppers	0.99492	0.994972	0.99531	0.99521	0.99449
Baboon	0.99521	0.99499	0.99413	0.99420	0.99491
Couple	0.99511	0.99425	0.99502	0.99432	0.99417
Boat	0.99414	0.99245	0.99324	0.99345	0.99417
Truck	0.99123	0.99421	0.99284	0.99241	0.99145
Airplane	0.99125	0.99142	0.99142	0.99187	0.99425
Tank	0.99511	0.99521	0.99545	0.99512	0.99524
Car and APCs	0.99352	0.99315	0.99322	0.99521	0.99421
Male	0.99212	0.99142	0.99123	0.99525	0.99245
Airport	0.99254	0.99469	0.99545	0.99452	0.99452

Table 2. Robustness (NC) results for various chaotic MSF without attacks.

Attacks	MSFs ($\alpha_1, \alpha_2, \alpha_3$)					
	(10,5,1)	(5,10,1)	(1,10,5)	(1,1,1)	(5,5,5)	Ref[25].
Cropping (Center, 20)	0.99412	0.99401	0.99412	0.99312	0.99412	0.9200
Cutting (10 rows)	0.99411	0.99421	0.99412	0.99381	0.99411	0.9822
Shearing (1, 0.2)	0.99423	0.99432	0.99388	0.99312	0.99401	0.9018
Translating (20, 20)	0.99445	0.99415	0.99414	0.99351	0.99434	0.9380
Shift (30)	0.99412	0.99451	0.99431	0.99374	0.99421	0.9907
Rotating (110)	0.99413	0.99442	0.99445	0.99312	0.99387	0.9479
Scaling (0.25, 4)	0.99431	0.99388	0.99421	0.99315	0.99451	0.9680
Median filter (3, 3)	0.99407	0.99415	0.99429	0.99301	0.99325	0.9974
Gamma Correction (0.8)	0.99444	0.99431	0.99415	0.99333	0.99424	0.9939
Wiener Filter (3, 3)	0.99414	0.99398	0.99381	0.99331	0.99421	0.9901
Histogram Equalization	0.99412	0.99354	0.99451	0.99311	0.99388	0.9311
Salt Peppers Noise (0.3)	0.99295	0.99221	0.99321	0.99244	0.99387	0.9353
Speckle Noise (0.3)	0.99011	0.99013	0.99011	0.99013	0.99121	0.9152
Gaussian Filter (0.3)	0.99213	0.99112	0.99101	0.99001	0.99215	0.9003
JPEG Compression (30)	0.99412	0.99315	0.99415	0.99251	0.99424	0.9930

Table 3. Robustness (NC) results for three MSFs under different attacks on the Pepper image.

outcomes of nearly 1. Eventually, we used three MSF matrices and five host images to depict the flexibility of the proposed schemes.

To evaluate the proposed scheme under different well-known attacks, Peppers image is used under three MSF matrices. Table 3 and 4 display the NC scores to the proposed scheme and compare them with another former scheme. Fifteen various geometrical and non-geometrical attacks used in image and signal processing were conducted on the watermarked images, then the embedded watermarks are extracted. One can see that the proposed scheme can effectively extract the embedded watermark under various attacks regardless of the MSFs values. NC scores of the proposed scheme are near 1, which that indicates the robustness is near ideal. Moreover, different MSFs values can produce high robustness against many well-known attacks. Unlike other schemes, the optimized MSF parameters can determine the value of imperceptibility and robustness. To show more efficiency of the proposed scheme, Figures 13 and 14 depict the extracted watermark and the watermarked images against the various attacks. One can see that the proposed scheme can extract the embedded watermark with lower distortions.

To compare the proposed watermarking scheme with other existing schemes, Table 5presents the PSNR imperceptibility values for multiple host images. The table highlights that the proposed scheme achieves high imperceptibility levels compared to other existing schemes such as[25,42]. Moreover, Table 6provides a comparison of the NC values of the proposed scheme with other existing schemes[30,41,44,59] under various geometric and non-geometric attacks. To ensure a fair comparison, several critical attacks, including Salt and Pepper, Gaussian noise, and Speckle noise, are conducted, and their results are shown in Table 7. The proposed scheme outperforms other existing schemes in terms of NC values, which indicates that the embedded watermark can be extracted with minimal distortion.

Attacks	MSFs ($\alpha_1, \alpha_2, \alpha_3$)					Ref[25].
	(10,5,1)	(5,10,1)	(1,10,5)	(1,1,1)	(5,5,5)	
Cropping (Center, 20)	0.99401	0.99412	0.99422	0.99201	0.99385	0.9340
Cutting (10 rows)	0.99388	0.99365	0.99345	0.99211	0.99412	0.9757
Shearing (1, 0.2)	0.99412	0.99412	0.99422	0.99212	0.99441	0.9130
Translating (20, 20)	0.99422	0.99421	0.99388	0.99232	0.99315	0.9470
Shift (30)	0.99444	0.99345	0.99412	0.99112	0.99245	0.9910
Rotating (110)	0.99342	0.99312	0.99380	0.99212	0.99354	0.9507
Scaling (0.25, 4)	0.99323	0.99454	0.99384	0.99304	0.99431	0.9720
Median filter (3, 3)	0.99358	0.99318	0.99342	0.99101	0.99322	0.9969
Gamma Correction (0.8)	0.99312	0.99415	0.99325	0.99111	0.99338	0.9956
Wiener Filter (3, 3)	0.99424	0.99454	0.99321	0.99211	0.993441	0.9892
Histogram Equalization	0.99421	0.99231	0.99314	0.99104	0.99401	0.9405
Salt Peppers Noise (0.3)	0.99211	0.99118	0.99265	0.98401	0.98888	0.9433
Speckle Noise (0.3)	0.98012	0.98875	0.98654	0.98011	0.98358	0.9277
Gaussian Filter (0.3)	0.99054	0.99241	0.99254	0.99011	0.99321	0.9878
Jpeg Compression (30)	0.99401	0.99421	0.99432	0.99325	0.99321	0.9965

Table 4. Robustness (NC) results for different chaotic MSF values under different attacks on the Peppers image.

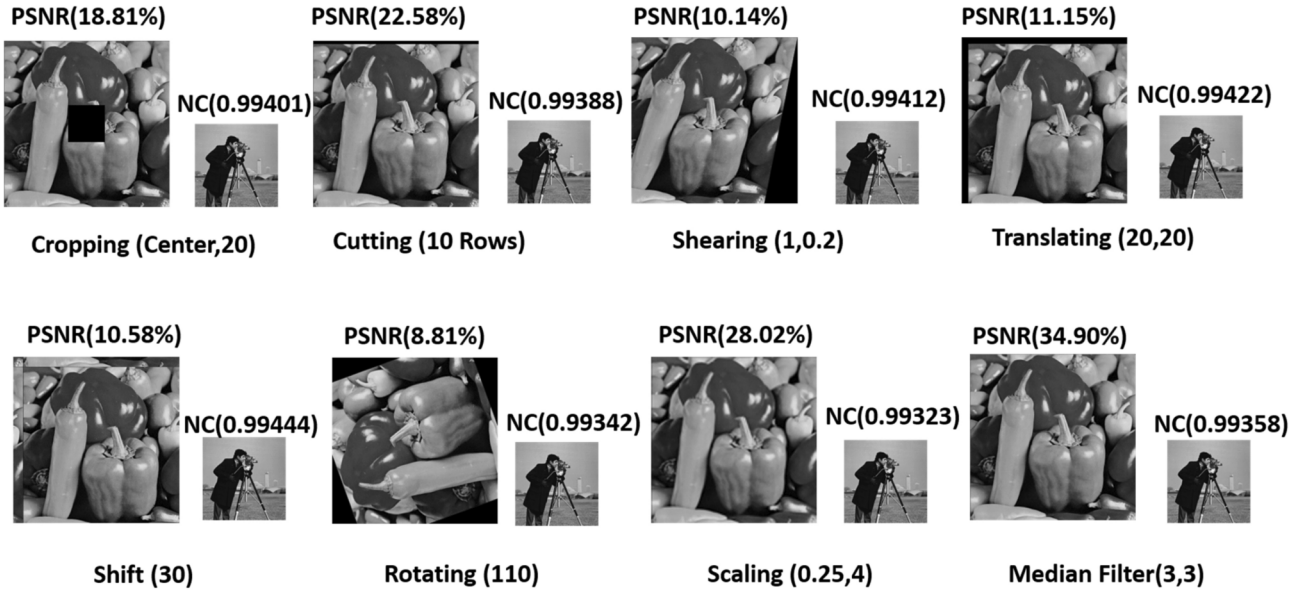

Fig. 13. First attacks against watermarked image and extracted watermark.

The proposed scheme's superior performance can be attributed to its strategy of embedding the image watermark in high-frequency sub-bands and combining 4-bit of LL_1 with 8-bit of the watermark image. This approach avoids the centralized embedding strategy in a single sub-band, resulting in minimal distortions in the recovered watermark image. Furthermore, Tables 8, 9, 10, 11, and 12illustrate the proposed scheme's robustness under various density and noise attacks. For comparison, two existing schemes[60]and[26] are used, and the proposed scheme outperforms them in terms of NC values under various density and noise attacks.

In summary, the proposed scheme achieves higher imperceptibility and better robustness under various attacks compared to other existing watermarking schemes. This is due to its effective embedding strategy and the combination of 4-bit of LL_1 with 8-bit of the watermark image, which helps to avoid significant distortions in the recovered watermark image.

FPP Analysis

A lot of digital images are created and published online, an image watermarking scheme is very important for copyright ownership protection of digital images. SVD image watermarking suffers from FPP issues and there

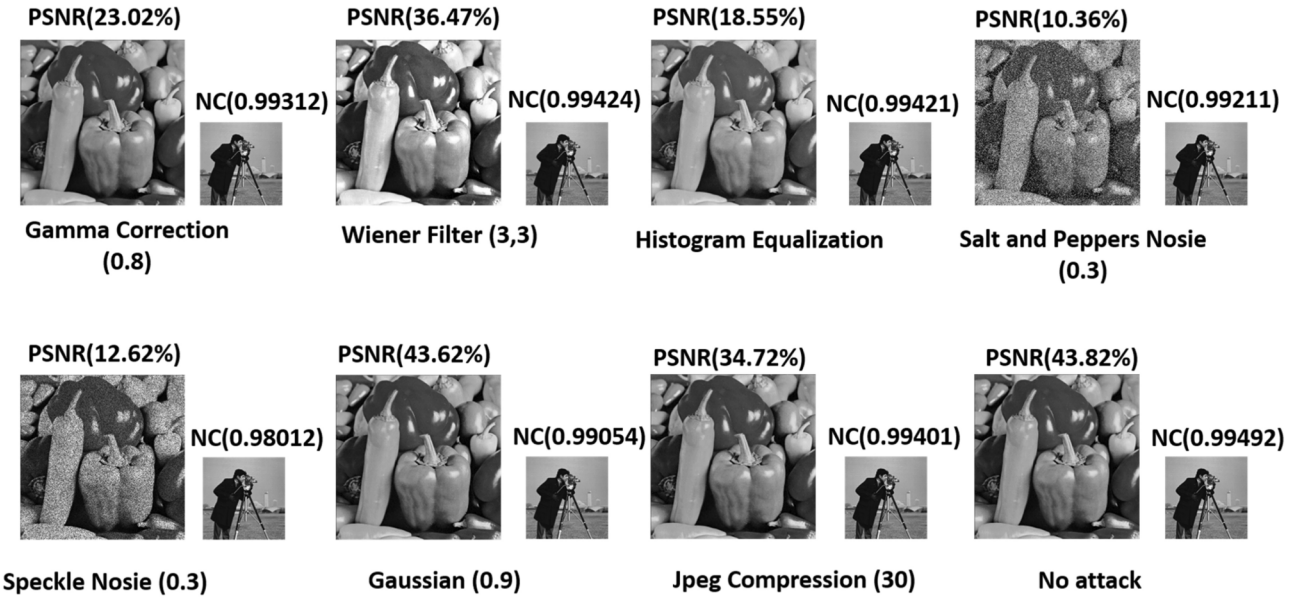

Fig. 14. Second group attacks against watermarked image and extracted watermark.

Test Image	Proposed scheme	Ref[25].	Ref[42].	Ref[27].
Airplane	**46.91**	42.9245	39.56	44.51
Peppers	**43.82**	42.9477	39.98	-
Baboon	37.37	**42.9159**	39.31	-
Couple	**43.98**	42.9322	39.63	43.90
Boat	43.25	42.9381	39.31	**44.39**

Table 5. Imperceptibility comparison between various schemes. (-) denotes no available result for the host image.

Attacks	Ref[59].	Ref[41].	Ref[44].	Ref[30].	Proposed sechme
Histogram Equalization	0.9934	0.9849	0.9664	**0.9982**	0.99412
Gaussian Filter	0.9849	0.9244	0.9358	0.9567	**0.99213**
JPEG Compression	**0.9991**	0.9954	0.9875	0.9942	0.99412
Gamma Correction	**0.9981**	0.9952	0.9585	0.9948	0.99444
Median Filter	0.9932	0.9894	0.9458	0.9903	**0.99407**
Cropping	0.9907	0.9592	0.5789	0.9878	**0.99412**
Shift	0.9934	0.9899	0.5435	0.9847	**0.99412**

Table 6. Robustness (NC) comparison under different attacks between various schemes.

Attacks	NC values				
	Ref[61].	Ref[62].	Ref[63].	Ref[53].	Proposed scheme
Salt and Pepper	0.9894	0.894	0.9736	0.9734	**0.9929**
Gaussian Noise	0.9762	0.969	0.9849	0.9841	**0.9921**
Speckle Noise	**0.9981**	0.989	0.9522	0.9275	0.9901

Table 7. Comparing NC values of the proposed schemes with other schemes.

Attack	NC		
	Proposed Scheme	Ref[60].	Ref[26].
Salat and Pepper 0.5	**0.99101**	0.6320	0.5870
Salat and Pepper 0.3	**0.99295**	0.6650	0.6800
Salat and Pepper 0.1	**0.99297**	0.7830	0.9460
Salat and Pepper 0.01	**0.99314**	0.9510	0.9710
Salat and Pepper 0.001	**0.99344**	0.9750	0.9950

Table 8. Salt and Pepper different noise attacks.

Attack	NC		
	Proposed Scheme	Ref[60].	Ref[26].
Speckle Noise 0.5	**0.97213**	0.6900	0.7020
Speckle Noise 0.3	**0.98012**	0.7190	0.7560
Speckle Noise 0.1	**0.98431**	0.8100	0.8740
Speckle Noise 0.01	**0.99014**	0.9510	0.9720
Speckle Noise 0.001	0.99314	0.9720	**0.9940**

Table 9. Speckle noise attacks.

Attack	NC		
	Proposed Scheme	Ref[60].	Ref[26].
Gaussian Noise 0.5	**0.98987**	0.6380	0.5890
Gaussian Noise 0.3	**0.99051**	0.6520	0.6190
Gaussian Noise 0.1	**0.99132**	0.7050	0.7400
Gaussian Noise 0.01	**0.99301**	0.8780	0.9360
Gaussian Noise 0.001	**0.99451**	0.9790	0.9820

Table 10. Gaussian noise attacks.

Attack	NC		
	Proposed Scheme	Ref[60].	Ref[26].
Median Filter (2, 2)	**0.99412**	0.9920	0.989
Median Filter (3, 3)	**0.99358**	0.9890	0.982
Median Filter (5, 5)	**0.99014**	0.9710	0.9500
Median Filter (7, 7)	**0.98987**	0.9510	0.9140
Median Filter (9, 9)	**0.98714**	0.9330	0.8820

Table 11. Median filter attacks.

are many schemes that have fallen on this issue[14,26,30]. To overcome or avoid the FPP attacks, the proposed system has conducted many successful security procedures as follows

- An attacker can embed his/her watermark in any digital image that is shared on WWW by using a different image watermarking scheme, and he/she can claim ownership of the watermarked image. Thus, CA is found as the database index to store the digital images and any related information of the ownership. In this proposed scheme, the secret key is stored in the CA and with the owner. To verify the ownership, the stored key, and the owner's key are matched to prove the copyright ownership. Other schemes used the authenticated data in the matching process, the authenticated data is embedded into the host image simultaneously with the embedded watermark image. Thus, in the extraction stage, the authenticated data is first extracted and then matched with stored authenticated data to prove the ownership. An attacker can embed his/her watermark image and authenticated data into the watermarked image by using an image watermarking scheme, and he/she can extract his/her watermark image and authenticated data, and claim ownership of the watermarked

Attack	NC		
	Proposed Scheme	Ref[60].	Ref[26].
JPEG compression Q = 5	**0.99105**	0.9520	0.9860
JPEG compression Q = 10	0.99208	0.9720	**0.9950**
JPEG compression Q = 20	0.99310	0.9830	**0.9980**
JPEG compression Q = 25	0.99389	0.9850	**0.9980**
JPEG compression Q = 30	0.99401	0.9870	**0.9980**
JPEG compression Q = 40	0.99410	0.9880	**0.9990**
JPEG compression Q = 50	0.99420	0.9900	**0.9990**
JPEG compression Q = 70	0.99430	0.9940	**0.9990**

Table 12. JPEG compression attacks.

image. Therefore, CA is a third-party database index to prove the ownership of digital images and protects the watermarked image and authenticated data.

- A secret key is a way to avoid extracting the fake watermark, whereby is used to be a secure scheme. It uses in a combination way that scrambled a matrix of the extracted 4-bit of LL_1, and it uses to generate chaotic variables to generate A matrix. The sorted I_s index of A that uses to scramble a 4-bit matrix of the LL_1. Without the secret key is hard to find the original 4-bit matrix to compare with 4-bit matrix of the watermarked image.
- A side information plays a role in SVD watermarking schemes, whereby singular S values do not hold the major geometrical contents of the digital image, S is easier to use in FPP attacks from other attackers. Thus, the type of side information has to play a role to avoid FPP attacks. W'_{LL} has major geometrical contents of the watermark image and it is encrypted by the matrix A and I_s with $\frac{M\times N}{4}$. Thus, without using the secret key, the encrypted W'_{LL} will generate a random watermark after applying inverse IWT.This analysis assumes that the secret key used in the proposed scheme is accessible to potential attackers. The purpose is to carefully study the security issues of the scheme, particularly in terms of its resilience against attacks even when the secret key is compromised. For this reason, the method of matching the secret key is not considered in this analysis. By assuming that the secret key is accessible, the analysis aims to identify any potential weaknesses or vulnerabilities in the scheme that could be exploited by attackers with knowledge of the secret key. This can help to improve the overall security of the scheme and make it more robust against potential attacks.
-
- **FPP Scenario 1:**Let us consider Peppers, a host image L, and two watermark images (Cameraman C and Woman W). The C watermark is embedded into L to produce the watermarked image LC, while another version of L is used as the host image, and W is embedded to produce another watermarked image, LW. The two schemes use different secret keys, and two LL side information are encrypted. When an attempt is made to extract the W of the LC using the side information of LW, or vice versa, the $C'LL$ values obtained are completely different from the $W'LL$ values. This occurs because two different secret keys will generate two chaotic matrices, and the LL sub-bands will be completely scrambled, producing only noise watermark images. This is depicted in Figure 15.
- **FPP Scenario 2:** The owner produced the new watermarked image LC, which the watermark is C and the host image L. An attacker uses the LC as the host image to embed the W watermark to produce a new watermarked image LC_W. Both secret keys are different in the two embedding processes, both encrypted LL sub-bands of the side information also are different. The attacker then tries to extract his/her watermark W from LC by using the secret key and the side information of the watermark LC_W. The attacker can extract W by the secret key LC_W because W'_{LL} is decrypted and has major image contents. However, The extracted 4-bit of LC is different from the extracted 4-bit of $W^{Extracted}$ because both secret keys are totally different and lead to scrambled matrices. The finding comparison is very low NC values. Thus, an attacker can not claim the ownership of W from LC as shown in Figure 16.
- **FPP Scenario 3:** In the proposed attack, the owner generates a watermarked image LC and keeps the secret key secure. An attacker, on the other hand, has access to an arbitrary image X, which does not have any watermark embedded in it. The attacker tries to extract the watermark C from X using the encrypted side information without having the secret key of LC. Since the attacker does not have the secret key of X, the side information is difficult to decrypt without the correct secret key. However, we assume that the attacker has the secret key of LC and uses it to decrypt the side information. Using the secret key, the attacker can extract the watermark image C from X with some distortions due to the different singular values of X on the watermarked image L. Moreover, the 4-bit of LL_X is extracted and compared with the 4-bit of the extracted watermark C. The resulting comparison yields very low NC values. As a result, the attacker cannot claim the ownership of X, as illustrated in Figure 17.

It can be inferred that the proposed watermarking scheme effectively resolves FPP-related issues that often occur when embedding in the singular values S of the host image. The primary factor that enables the proposed scheme to overcome FPP is the secret key. The secret key ensures that the algorithm is secure and the original watermark cannot be easily extracted. Thus, the proposed scheme can be likened to a cryptographic algorithm that relies on the secret key in its design. Another key factor in the proposed watermarking scheme is the 4-bit extracted from the host image, which is then incorporated into the watermark image. The matching process between the two

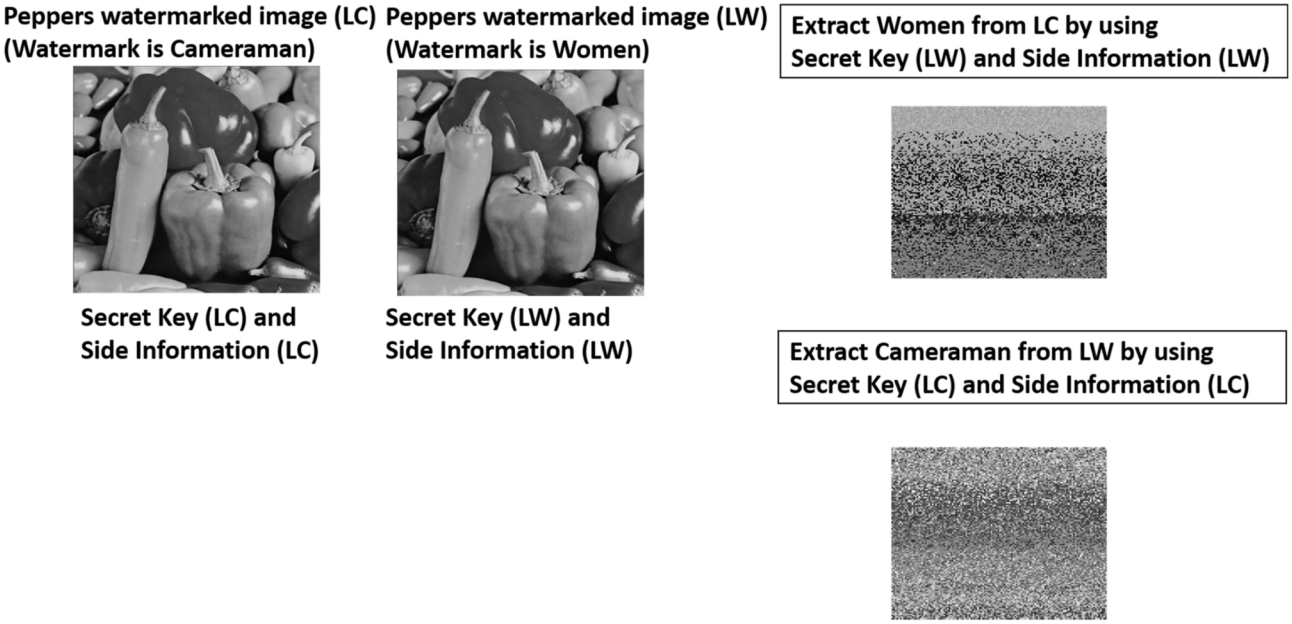

Fig. 15. Resistance against FPP attack 1.

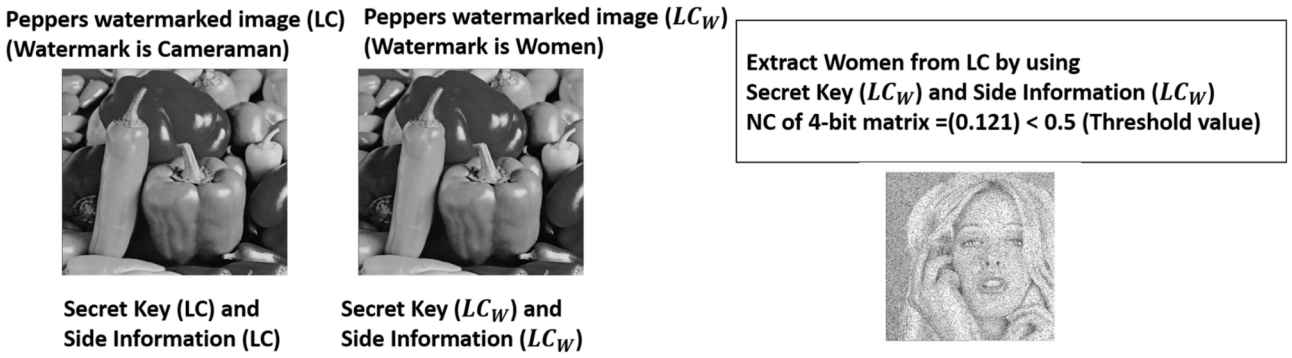

Fig. 16. Resistance against FPP attack 2.

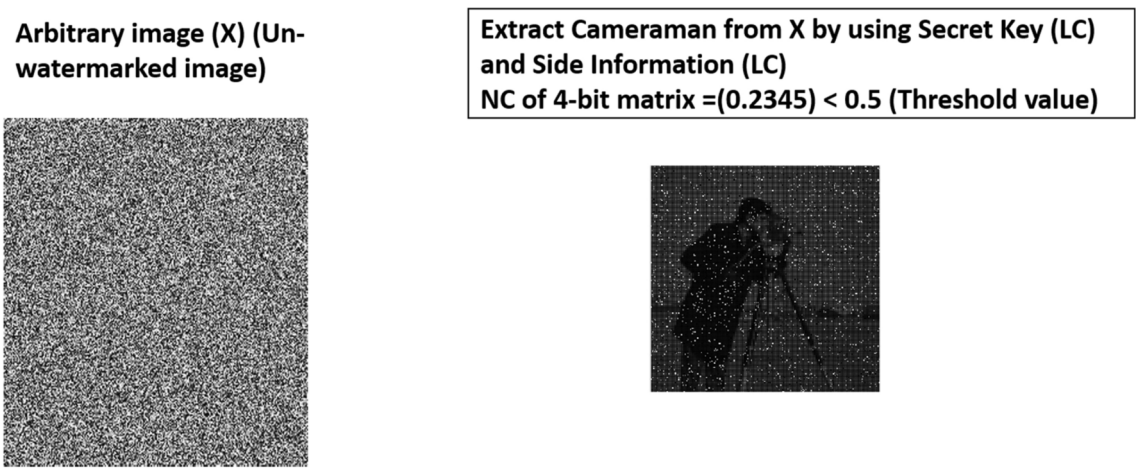

Fig. 17. Resistance against FPP attack 3.

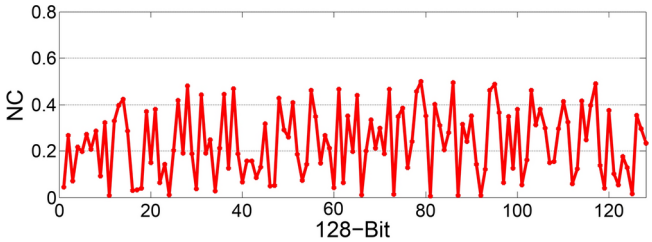

Fig. 18. Secret key sensitivity of the proposed scheme.

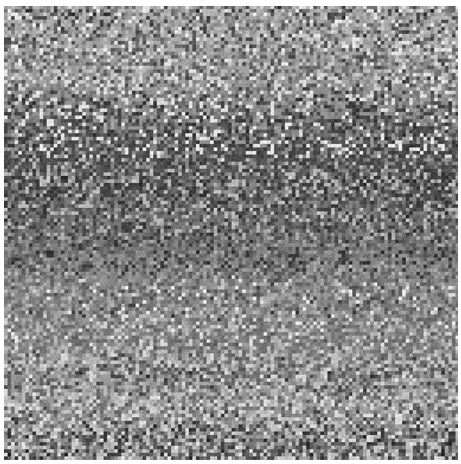

Fig. 19. Extracted noise watermark image via toggling one-bit of the secret key.

extracted 4-bit is regulated by the chaotic maps and the secret key. As a result of the scrambling algorithm and random chaotic points, any modification to the secret key will result in an entirely new scrambled 4-bit.

In conclusion, the proposed scheme overcomes FPP issues by leveraging a secure secret key and a robust matching process between extracted bits. The combination of the secret key and chaotic maps ensures that any alteration to the key will lead to a completely different scrambled 4-bit. This approach provides an extra layer of security and makes the watermarking scheme more difficult to breach.

Secret key sensitivity

The proposed watermarking scheme employs a secret key that plays a crucial role in the security of the system. Even a slight modification in the secret key generates new chaotic variables and a completely different watermarked image. Hence, it is essential to ensure that the secret key is highly sensitive to small changes to guarantee the security of the watermarked image. Based on section 3.1, any minute change to the secret key produces entirely different chaotic points, resulting in different MSF matrices and encrypted side information. Therefore, the slightest modification leads to significant variations in the watermarked image, making it challenging to extract the correct watermark image using an incorrect secret key.

To investigate the proposed scheme's sensitivity to the secret key, we perform a normalized correlation (NC) experiment to measure the similarity between the extracted watermarks and the original watermark after toggling the secret key's bits. The secret key K_0 generates the watermarked image IW, where I and W represent the host image and the watermark image, respectively. To test the scheme's sensitivity, we generate a new set of secret keys $K_i, i = 1, 2, 3, ..., 128$, by toggling each of the 128-bit positions of K_0. Next, each new secret key is used in the extraction process, and we calculate the NC value between the extracted watermark under the K_i key and the original watermark. Figure 18 displays the NC values obtained for 128 cases.

The results of the experiment demonstrate that even a small one-bit change to the secret key can significantly affect the extracted watermarks. Figure 19 shows the extracted watermark image using an incorrect secret key, which is indecipherable and filled with noise. Hence, we can conclude that the proposed watermarking scheme is highly sensitive to any modification in the secret key, making it more secure against attacks.

In summary, the proposed watermarking scheme utilizes a secret key that is highly sensitive to tiny changes, making it more secure. The NC experiment results reveal that even a one-bit change to the secret key leads to a significantly different watermarked image. Therefore, the proposed scheme provides robust protection against various attacks, making it a suitable choice for secure watermarking applications.

Flexibility

In an image watermarking scheme, flexibility is a very significant property, different embedding capacities are needed to be a flexible scheme. The proposed scheme can embed the watermark images into three sub-bands at the same time, each sub-band decomposed by SVD transform, and the singular values are selected to complete the procedure. We can embed the same watermark image into three sub-bands or we can embed different watermark images in three second-level of the host image. Four sub-bands of the first level of the host image can transform into 16 sub-bands. Therefore, the proposed scheme can embed multi-watermark images in the host image. The way of embedding is just to select which sub-band to achieve the maximum capacity and does not reduce NC and PSNR scores.

We embed two different watermark images into six sub-bands of the host image. We select LL_{1HL_2}, LL_{1LH_2}, and HH_{1HL_2} for the second watermark image. We calculate the NC and PSNR values for the extracted watermarks and the watermarked image. The PSNR score of the watermarked image is (40.24) and the NC scores of the two watermark images are (0.99246) and (0.99123). The results indicate that the proposed scheme has high scores for imperceptibility and robustness even though the embedding is conducted into six sub-bands at the same time. Thus, the proposed scheme has the flexibility to handle different watermark images as well as the potential to embed into six sub-bands.

Computational complexity

In this section, computational complexity analysis of the proposed scheme is provided in terms of the time required for embedding and extraction. The proposed scheme has a set of stages in the embedding process that includes combination, scrambling, MSF generation, and the embedding itself. The extraction process has two stages: decryption and extraction. Again, embedding requires more time than extraction because the embedding process needs to reconstruct the host image after inserting the watermark. On the other hand, extraction focuses on reconstructing the watermark image for which some of the data are already available in the side information.

For comparison with the proposed scheme, all schemes use IWT as one of their design components. A 512×512 host image and a 256×256 watermark image were used for efficiency comparisons. The embedding time, extraction time, and total time are shown in Table 13. The number of optimization rounds is selected based on the state of the art, which is 12 rounds[64](most schemes based on optimization algorithms set a limit of 25 rounds). Thus, estimate the total time for embedding, and the execution time of the scheme is multiplied by 12. All results are the average of 10 executions of each scheme. In contrast to the existing scheme mentioned in[65], which requires a significant amount of time (specifically 22.83 seconds) to execute the embedding process (excluding the time for training machine learning), our proposed scheme demonstrates faster processing time. Additionally, our scheme eliminates the need for training or searching for optimized MSF values.

The two selected schemes were implemented on the same computer (2.6 GHz CPU, 6 GB RAM, 64-bit Windows 10) using MATLAB version 2012b. Results in Table 13 show that the proposed scheme has a faster embedding algorithm, whereas the benchmark schemes are faster in terms of extraction than the proposed scheme. The total execution time (inclusive of both embedding and extraction) of the proposed scheme is lower than the other schemes. It is evident from the results that the proposed scheme greatly outperforms the schemes based on optimization algorithms in terms of embedding time which makes it nearly three times faster than the other schemes when both embedding and extraction are taken into consideration.

Real-World images

In this experiment, three real-world images were selected as the host images, and the Cameraman was selected as a watermark image for the three host images. All images are color images with three channels, red, green, and blue. The grayscale watermark image is embedded into the red, green, and blue channels of the host image. This experiment is designed to showcase the applicability of the proposed scheme to real-world images. Figure 20 shows the host and watermark images. Table 14 provides the PSNR and NC results for each channel. One can see that the results are close to the standard images that were used previously. This confirms that the proposed scheme has the same effect on real-world images and can be used for real-life applications.

Comparative analysis

The proposed scheme has presented two new ideas in a hybrid SVD-based image watermarking scheme, the combination way is conducted to protect the watermark image against different attacks. The side information is encrypted to increase the security of the proposed scheme and extra way to avoid FPP issues. This scheme focuses on the make the key secret with the owner not allowing to any attacker extract a fake watermark or use side information in a fake extraction strategy. The high-frequency matrices of the watermark are used to embed into the singular values of the second-level sub-bands of the host image with three MSF chaotic matrices. In addition, the secret key is high sensitivity to a small change and leads to extracting a fake watermark. Finally, the proposed

Scheme	Embedding time (s)	Extraction time (s)	Total time (s)
Proposed scheme	0.87	0.68	1.55
Ref[25].	$(0.36 \times 12 = 4.32)$	0.35	4.67
Ref[64].	$(0.45 \times 12 = 4.5)$	0.32	4.82

Table 13. Computational time evolution of the proposed scheme with other schemes.

Fig. 20. Real-world host images and the Cameraman watermark image.

Image	Red		Green		Blue	
	PSNR	NC	PSNR	NC	PSNR	NC
USM	42.12	0.99315	40.15	0.99215	39.85	0.99365
Penang	37.84	0.99415	38.45	0.99410	39.51	0.99301
School	43.85	0.99462	41.98	0.99412	42.98	0.99432

Table 14. imperceptibility and robustness results for the real-world images.

Reference	Embedding Sub-Bands	Type of Transforms	Watermark Size	Scaling Factor	Solve FPP
Proposed Scheme	LL_2 and HH_2	IWT+SVD	Equal to or smaller than host image	MSF (Chaotic)	Yes
Ref[23].	DC	DCT+SVD	64×64	MSF(DE)	Yes
Ref[14].	HL and LH	DWT+SVD	256×256 and 12 characters	SSF	No
Ref[27].	LL_3 and HH_3	DCT+DWT+SVD	128×128	MSF (PSO)	Yes
Ref[28].	All	RT+DWT+SVD	33×33	SSF	No
Ref[30].	ALL	DWT+SVD	256×256	MSF (PSO)	Yes
Ref[67].	LH_3	DWT+SVD	32×32	MSF (MOACO)	Yes
Ref[63].	LL_2	DWT+DCT+SVD	256×256	SSF	No
Ref[36].	HH	DWT+SVD	256×256	-	Yes
Ref[41].	LL_3 and HH_3	DWT+SVD+HVS	64×64	(MSF) DE	Yes
Ref[68].	All	DWT+SVD	256×256	(MSF) SDE	Yes
Ref[66].	All	RSWT +SVD	512×512	SSF	No

Table 15. Comparative analysis of SVD-based watermarking schemes.

scheme is based on some factories that lead to more robustness and security, it has a high imperceptibility and robustness.

Other existing schemes used SVD in their designs[25,27,31,32,66]. These schemes handle FPP issues by embedding one of the singular vectors or principal components. However, these embedding strategy is not robust enough against some well-known attacks[25,31,32]. The proposed scheme has an extra security way by using encryption side information to avoid the effect of well-known attacks. Table 15 displays a set of factors to compare the proposed scheme with other existing watermarking schemes. It can be noted that the proposed scheme successfully mitigates the problems associated with FPP and exhibits a superior degree of robustness when compared to other schemes. The PSNR and NC values of the proposed scheme are very high and the proposed scheme can embed different watermarks into six sub-bands.

Table 16 shows a comparison of the average NC values among the proposed scheme and other existing schemes. The NC values measure the similarity between the original and extracted watermark images, with higher values indicating better performance in terms of preserving the integrity and visibility of the embedded watermark.

Analyzing the table, it is evident that the proposed scheme consistently achieves high NC values across different image processing operations, including Salt and Pepper noise, Gaussian noise, Median filter, Cropping, and JPEG compression. This suggests that the proposed scheme exhibits robustness and can effectively withstand various types of attacks, maintaining the quality and visibility of the watermarked images.

	Salat and Pepper	Gaussian Noise	Median Filter	Cropping	JPEG Compression
Proposed Scheme	0.992	0.992	0.993	0.990	0.999
Ref[54].	0.951	0.974	0.988	0.791	0.994
Ref[60].	0.632	0.638	0.989	-	0.952
Ref[26].	0.995	0.619	0.989	-	0.998
Ref[51].	0.992	0.986	0.994	0.991	0.993
Ref[16].	0.997	0.997	0.997	0.997	0.997
Ref[69].	0.2150	0.991	0.994	0.737	0.997
Ref[70].	0.114	0.112	0.994	0.479	0.428
Ref[71].	0.686	0.816	0.969	0.998	0.991
Ref[72].	0.951	0.907	0.991	-	0.989
Ref[65].	0.885	0.973	0.988	-	0.992
Ref[73].	0.979	0.952	0.984	-	0.921

Table 16. Comparison of average NC among the proposed scheme and other schemes.

Comparing the proposed scheme with the existing schemes, several interesting observations can be made:

- Ref[54]. demonstrates relatively high NC values, particularly in Gaussian noise and Median filter operations. However, it falls short in Salt and Pepper, Cropping, and JPEG compression, where the proposed scheme outperforms it. This indicates that the proposed scheme offers better resilience against these types of attacks.
- Ref[60]. exhibits lower NC values in most operations, suggesting a potential degradation in image quality and visibility. Additionally, it lacks data for the Cropping operation, making it difficult to assess its performance comprehensively. Similarly, Ref[26]. achieves high NC values only in the Salt and Pepper operation, but lower values in other operations. This indicates a limitation in its ability to withstand various attacks.
- Ref[51]. demonstrates competitive performance across all operations, with high NC values comparable to the proposed scheme. It showcases effectiveness in preserving the integrity and visibility of watermarked images. Similarly, Ref[16]. achieves consistently high NC values, suggesting its robustness and reliability in different attack scenarios.
- On the other hand, some referenced schemes, such as Ref[69]., Ref[70]., Ref[71]., Ref[72]., and Ref[65]., exhibit significantly lower NC values across multiple operations. This implies a potential loss of image quality or vulnerability to attacks in those schemes. Ref[73]. achieves moderate NC values but falls behind the proposed scheme in terms of overall performance.Overall, the analysis of Table 16 indicates that the proposed scheme demonstrates favorable performance, consistently achieving high NC values across various image processing operations. It outperforms most of the referenced schemes in terms of preserving the integrity and visibility of watermarked images. However, a few referenced schemes exhibit competitive performance in specific operations. Further research and analysis are necessary to understand the underlying factors contributing to the variations in performance among the schemes and to determine the specific strengths and weaknesses of each scheme in different attack scenarios.

In the existing scheme[51], we used chaotic maps to generate MSF values and to encrypt the watermark image before the embedding process started. The secret key is extracted from the host image and watermark image to be unique for both images. We used a novel method to encrypt the watermark image by converting it to another random matrix, which is helping in the protection of the embedded watermark image under the different well-known attacks. In this proposed scheme, the secret key is not unique to the host and watermark image, it is a flexible one for the owners, and he/she selects any suitable secret key. The chaotic points are used to scramble the 4-bit of the LL sub-band of the host image, three MSF parameters are generated by chaotic points, and the side information is encrypted after the embedding is conducted. Therefore, this scheme has essential differences on the[51].

In our previous scheme[16], we utilized an eight-bit plane from the watermark image and embedded it within various sub-bands of the host image. The embedding process was lightweight, with only one-bit values being embedded. Consequently, the capacity was limited to the number of ones, and the extracted watermark image remained resilient against various geometric attacks. As a result, our previous scheme demonstrated higher scores compared to both other schemes and our new proposed scheme. However, the advantage of our new proposed scheme lies in its ability to protect the extracted watermark image. In this scheme, the new watermark (12-bit)is embedded in the host image, allowing for its extraction and verification of ownership without relying solely on encrypting the watermark image or employing additional techniques for protection.

Three new schemes are formulated to address challenges including the FPP and balancing imperceptibility and robustness, with each scheme possessing its own set of advantages and disadvantages. It is crucial to conduct a comparison of these schemes in order to highlight their distinctions. The strengths and limitations of the three schemes are presented in Table 17.

Table 17 summarizes the advantages and disadvantages of three schemes based on different factors, such as the secret key, embedding strategy, and robustness against FPP attacks. Each scheme is presented in a separate row, with its associated strengths and limitations listed in the respective columns.

Scheme	Advantages	Disadvantages
Ref[51].	The secret key is derived from both the host and watermark images. The watermark image is transformed into a noise image to enhance its security.	The secret key is less flexible in terms of changes.
Ref[16].	The embedding process is generated using bit-planes, and multiple sub-bands are utilized for embedding. The embedding process is randomized, and a flexible secret key is used.	The embedding process is repeated eight times, which may affect the image quality.
The Proposed Scheme	A part of the host image is embedded in the watermark image, and the 4-bit of LL sub-band of the host image is extracted to prevent FPP attacks. The watermark image is transformed into the frequency domain before embedding. The side information is encrypted, and the embedding process is repeated four times.	The side information is relatively large.

Table 17. Comparison of the Strengths and Limitations of Three Proposed Schemes.

The first scheme, Ref[51]., extracts the secret key from the host and watermark image and encrypts the watermark image by converting it into a noise image. Although this scheme offers good robustness against FPP attacks, its secret key is not as flexible as the other schemes, which may limit its practical applications.

The second scheme, Ref[16]., utilizes a flexible secret key and generates the embedding strategy using bit-planes. It also uses various sub-bands and random embedding, which contributes to its good imperceptibility and robustness. However, its embedding process is repeated eight times, which can increase the computational complexity.

Finally, the proposed scheme combines various techniques, including the use of a watermark image that contains a part of the host image and the extraction of a hash value to avoid FPP attacks. The scheme also encrypts the side information and uses the frequency domain for embedding. Moreover, the scheme repeats the embedding process four times, which reduces the risk of false positives and improves robustness. However, the side information may be large, which can affect its practicality.

Discussion

In the proposed scheme, IWT and SVD transforms are used due to their simple mathematical computations and to achieve a good trade-off between imperceptibility and robustness. Chaotic maps are used in three parts to make the proposed scheme secure and flexible. The proposed scheme has some advantages which include the following:

- The proposed scheme incorporates a secret key which is utilized for generating MSF parameters, scrambling LL_1, and encrypting the LL of the side information. Additionally, the secret key plays a crucial role in the matching process, thereby ensuring protection against any potential attacks aimed at claiming ownership of the watermarked image.
- The embedding process is carried out on both the LL and HH sub-bands of the host image to attain a desirable balance between imperceptibility and robustness.
- The capacity of the watermark image is increased by embedding it in three high-frequency sub-bands.
- α_i parameters are generated by using chaotic points of the enhanced chaotic maps and C scale parameter. Even without optimization search algorithms, the chaotic watermarking image scheme can achieve a good trade-off between imperceptibility and robustness.
- To avoid FPP issues, the side information W'_{LL} is encrypted by the secret key and chaotic maps. Moreover, the 4-bit of $LL_1(b_0, b_1, b_2, b_3)$ is added to the LSB of the pixel values of the watermark image to increase the security of the watermark image against the different distortion methods. In addition, the secret key is kept with the owner and CA to stop all FPP attacks and protect the watermarked image from any other cyberattacks.
- The scramble operation plays a crucial role in three stages of the embedding process. Firstly, it is applied to the 4-bit extracted from the sub-band (LL) of the host image. Secondly, it is used to scramble the newly combined watermark image along with the 4-bit extracted. Finally, it is utilized in the encryption stage to encrypt the side information.
- The combination of 4-bit sub-band extraction from the host image and the watermark image offers additional benefits, such as safeguarding the watermark from distortions and enabling the embedding of host image data after scrambling. This contributes to establishing ownership rights effectively.
- The 'Haar' wavelet transform in IWT employs integer coefficients, eliminating truncation issues and round-off errors. This results in enhanced image resolution.Although the proposed scheme has several advantages, it also has some limitations, including:
-
- It should be noted that IWT and SVD transforms may not be universally applicable to all types of digital images. There exist various types of digital images such as JPEG, PNG, GIF, BMP, TIFF, RAW, SVG, EPS, PSD, and AI. To explore the use of these transforms for all image types, it would be necessary to investigate their effectiveness with each type of frequency transform.
- While the proposed scheme overcomes security issues in existing schemes through encryption and chaotic maps, the computational complexity of the multiple SVD watermarking scheme may increase for multiple watermarking images.
- Another type of attack that can occur is a collusion attack, where a group of attackers works together to remove the embedded watermark image. This type of attack may limit the effectiveness of the proposed scheme in situations where collusion attacks are likely to occur. Each attack has its own unique method of targeting

the watermarked image.In Table 1, findings suggest that the choice of MSF values is crucial in achieving high imperceptibility of digital images, as it affects the quality of the watermarked image. The table presented as Table 2 displays the NC results for diverse chaotic MSF under non-attack conditions for various test images. Each MSF is identified by three parameters ($\alpha_1, \alpha_2, \alpha_3$), and the table compares the NC values obtained by applying different parameter sets for each image. The outcomes reveal that the proposed method can achieve high NC scores and can effectively retrieve the embedded watermark image. Nevertheless, the embedding approach relying on singular values suffers from a limited capacity, which we address by increasing the number of sub-bands utilized in the embedding process.

Our proposed scheme overcomes FPP issues through the use of two factors: the secret key and 4-bit extracted values. The secret key plays a significant role in providing security by making it difficult to extract the embedded watermark without knowledge of the secret key. This results in the proposed scheme acting as a cryptographic algorithm, where the secret key is the main component in its design and functionality. Another factor used to enhance the proposed scheme is the 4-bit values extracted from the host image, which are controlled by chaotic behaviors and secret keys. This makes it challenging to attack or tamper with the embedded watermark. Additionally, the scrambling algorithm and random chaotic points make any changes to the secret key result in a new scrambled 4-bit value, further improving the algorithm's resistance to FPP.

When compared to other existing schemes, the majority of them employ AI optimization algorithms to generate MSF parameters. However, these schemes require a substantial amount of time in the embedding algorithm as they need multiple rounds to obtain optimal MSF parameters. This means that the embedding scheme needs to be executed many times before arriving at the optimal solution. Conversely, extraction is faster since it only needs to be executed once with the optimal MSF as side information. In contrast, the proposed scheme requires less time than schemes based on optimization algorithms.

Conclusion

This paper proposes a new image watermarking scheme that utilizes IWT, SVD, and a chaos model. The secret key was used to generate chaotic variables, which are used to iterate the chaotic maps to generate chaotic sequences. Three MSF matrices were generated without optimization algorithms. The combination process was used to protect the watermark and prove ownership. The second-level IWT was applied on the LL_1 and HH_1 sub-bands to attain the high compromise between robustness and imperceptibility. Three high-frequency sub-bands of the watermark image were embedded into the singular values of the three sub-bands under the control of chaotic MSF values. To protect the side information against any distortion attacks, the side information was encrypted based on chaotic maps. The proposed scheme demonstrated a good compromise between robustness and imperceptibility, high sensitivity to a small change to a secret key, and overcoming FPP attacks by the stored secret key in the third party. Furthermore, the proposed scheme has highly flexible and can embed two different watermark images. Finally, The proposed scheme has effectively achieved the security and capacity demands of a blind watermarking scheme. In future work, we will incorporate the proposed scheme into the development and evaluation of adaptive watermark embedding strategies that can dynamically adjust the watermarking process based on image characteristics and content.

Data availability

The data supporting the findings of this study are available upon reasonable request. Interested researchers may contact Dr. Moatsum Alawida at moatsum.alawida@adu.ac.ae for access to the dataset.

Received: 15 January 2025; Accepted: 24 February 2025
Published online: 28 February 2025

References

1. Wang, Z. *et al.* Data hiding with deep learning: a survey unifying digital watermarking and steganography. *IEEE Transactions on Computational Social Systems* (2023).
2. Aberna, P. & Agilandeeswari, L. Digital image and video watermarking: methodologies, attacks, applications, and future directions. *Multimedia Tools and Applications* **83**, 5531–5591 (2024).
3. Soualmi, A., Laouamer, L. & Adel, A. A blind watermarking approach based on hybrid imperialistic competitive algorithm and surf points for color images' authentication. *Biomedical Signal Processing and Control* **84**, 105007 (2023).
4. Dhar, S. & Sahu, A. K. Digital to quantum watermarking: A journey from past to present and into the future. *Computer Science Review* **54**, 100679 (2024).
5. Sahu, A. K. & Swain, G. Information hiding using group of bits substitution. *International Journal on Communications Antenna and Propagation* **7**, 162–167 (2017).
6. Wang, J. et al. *Invisible adversarial watermarking: A novel security mechanism for enhancing copyright protection* (ACM Transactions on Multimedia Computing, Communications and Applications, 2024).
7. Soualmi, A., Laouamer, L. & Alti, A. A novel intelligent approach for color image privacy preservation. *Multimedia Tools and Applications* 1–22 (2024).
8. Sahu, A. K. A logistic map based blind and fragile watermarking for tamper detection and localization in images. *Journal of Ambient Intelligence and Humanized Computing* **13**, 3869–3881 (2022).
9. Sahu, M., Padhy, N., Gantayat, S. S. & Sahu, A. K. Shadow image based reversible data hiding using addition and subtraction logic on the lsb planes. *Sensing and Imaging* **22**, 7 (2021).
10. Amrutha, M. & Kannammal, A. A new highly fractal 1d-chaotic map-based novel encryption on hvs-based watermarked fundus images for 2-level security in teleophthalmology applications. *Physica Scripta* **98**, 125118 (2023).
11. Soualmi, A., Alti, A. & Laouamer, L. An imperceptible watermarking scheme for medical image tamper detection. *International Journal of Information Security and Privacy (IJISP)* **16**, 1–18 (2022).
12. Mohammed, A. O., Hussein, H. I., Mstafa, R. J. & Abdulazeez, A. M. A blind and robust color image watermarking scheme based on dct and dwt domains. *Multimedia Tools and Applications* **82**, 32855–32881 (2023).

13. Zhou, N.-R., Tong, L.-J. & Zou, W.-P. Multi-image encryption scheme with quaternion discrete fractional tchebyshev moment transform and cross-coupling operation. *Signal Processing* **211**, 109107. https://doi.org/10.1016/j.sigpro.2023.109107 (2023).
14. Anand, A. & Singh, A. An improved dwt-svd domain watermarking for medical information security. *Computer Communications* (2020).
15. Kumar, C., Singh, A. K. & Kumar, P. Dual watermarking: An approach for securing digital documents. *Multimedia Tools and Applications* 1–16 (2019).
16. Alshoura, W. H., Zainol, Z., Teh, J. S. & Alawida, M. An fpp-resistant svd-based image watermarking scheme based on chaotic control. *Alexandria Engineering Journal* **61**, 5713–5734. https://doi.org/10.1016/j.aej.2021.10.052 (2022).
17. Hsu, L.-Y. & Hu, H.-T. A reinforced blind color image watermarking scheme based on schur decomposition. *IEEE Access* **7**, 107438–107452 (2019).
18. Abdulrahman, A. K. & Ozturk, S. A novel hybrid dct and dwt based robust watermarking algorithm for color images. *Multimedia Tools and Applications* **78**, 17027–17049 (2019).
19. Ali, M., Ahn, C. W. & Pant, M. An efficient lossless robust watermarking scheme by integrating redistributed invariant wavelet and fractional fourier transforms. *Multimedia Tools and Applications* **77**, 11751–11773 (2018).
20. Najafi, E. & Loukhaoukha, K. Hybrid secure and robust image watermarking scheme based on svd and sharp frequency localized contourlet transform. *Journal of information security and applications* **44**, 144–156 (2019).
21. Makbol, N. M., Khoo, B. E. & Rassem, T. H. Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics. *IET Image processing* **10**, 34–52 (2016).
22. Roy, S. & Pal, A. K. A robust blind hybrid image watermarking scheme in rdwt-dct domain using arnold scrambling. *Multimedia Tools and Applications* **76**, 3577–3616 (2017).
23. Ali, M., Ahn, C. W. & Pant, M. A robust image watermarking technique using svd and differential evolution in dct domain. *Optik-International Journal for Light and Electron Optics* **125**, 428–434 (2014).
24. Singh, A. K. Improved hybrid algorithm for robust and imperceptible multiple watermarking using digital images. *Multimedia Tools and Applications* **76**, 8881–8900 (2017).
25. Makbol, N. M., Khoo, B. E., Rassem, T. H. & Loukhaoukha, K. A new reliable optimized image watermarking scheme based on the integer wavelet transform and singular value decomposition for copyright protection. *Information Sciences* **417**, 381–400 (2017).
26. Makbol, N. M. & Khoo, B. E. A new robust and secure digital image watermarking scheme based on the integer wavelet transform and singular value decomposition. *Digital Signal Processing* **33**, 134–147 (2014).
27. Zhang, L. & Wei, D. Dual dct-dwt-svd digital watermarking algorithm based on particle swarm optimization. *Multimedia Tools and Applications* **78**, 28003–28023 (2019).
28. Rastegar, S., Namazi, F., Yaghmaie, K. & Aliabadian, A. Hybrid watermarking algorithm based on singular value decomposition and radon transform. *AEU-International Journal of Electronics and Communications* **65**, 658–663 (2011).
29. Makbol, N. M., Khoo, B. E. & Rassem, T. H. Security analyses of false positive problem for the svd-based hybrid digital image watermarking techniques in the wavelet transform domain. *Multimedia Tools and Applications* **77**, 26845–26879 (2018).
30. Run, R.-S., Horng, S.-J., Lai, J.-L., Kao, T.-W. & Chen, R.-J. An improved svd-based watermarking technique for copyright protection. *Expert Systems with applications* **39**, 673–689 (2012).
31. Jain, C., Arora, S. & Panigrahi, P. K. A reliable svd based watermarking schem. arXiv preprint arXiv:0808.0309 (2008).
32. Liu, R. & Tan, T. An svd-based watermarking scheme for protecting rightful ownership. *IEEE transactions on multimedia* **4**, 121–128 (2002).
33. Loukhaoukha, K. & Chouinard, J.-Y. Hybrid watermarking algorithm based on svd and lifting wavelet transform for ownership verification. In *2009 11th Canadian Workshop on Information Theory*, 177–182 (IEEE, 2009).
34. Zebbiche, K., Khelifi, F. & Loukhaoukha, K. Robust additive watermarking in the dtcwt domain based on perceptual masking. *Multimedia Tools and Applications* **77**, 21281–21304 (2018).
35. Loukhaoukha, K., Chouinard, J.-Y. & Taieb, M. H. Optimal image watermarking algorithm based on lwt-svd via multi-objective ant colony optimization. *Journal of Information Hiding and Multimedia Signal Processing* **2**, 303–319 (2011).
36. Gupta, A. K. & Raval, M. S. A robust and secure watermarking scheme based on singular values replacement. *Sadhana* **37**, 425–440 (2012).
37. Araghi, T. K., Abd Manaf, A. & Araghi, S. K. A secure blind discrete wavelet transform based watermarking scheme using two-level singular value decomposition. *Expert Systems with Applications* **112**, 208–228 (2018).
38. Sreenivas, K. & Kamkshi Prasad, V. Fragile watermarking schemes for image authentication: a survey. *International Journal of Machine Learning and Cybernetics* **9**, 1193–1218 (2018).
39. Zear, A., Singh, A. K. & Kumar, P. A proposed secure multiple watermarking technique based on dwt, dct and svd for application in medicine. *Multimedia tools and applications* **77**, 4863–4882 (2018).
40. Roy, S. & Pal, A. K. An svd based location specific robust color image watermarking scheme using rdwt and arnold scrambling. *Wireless Personal Communications* **98**, 2223–2250 (2018).
41. Ali, M., Ahn, C. W. & Siarry, P. Differential evolution algorithm for the selection of optimal scaling factors in image watermarking. *Engineering Applications of Artificial Intelligence* **31**, 15–26 (2014).
42. Wang, J., Peng, H. & Shi, P. An optimal image watermarking approach based on a multi-objective genetic algorithm. *Information Sciences* **181**, 5501–5514 (2011).
43. Zhou, N. R., Luo, A. W. & Zou, W. P. Secure and robust watermark scheme based on multiple transforms and particle swarm optimization algorithm. *Multimedia Tools and Applications* **78**, 2507–2523 (2019).
44. Aslantas, V. An optimal robust digital image watermarking based on svd using differential evolution algorithm. *Optics Communications* **282**, 769–777 (2009).
45. Arsalan, M., Qureshi, A. S., Khan, A. & Rajarajan, M. Protection of medical images and patient related information in healthcare: Using an intelligent and reversible watermarking technique. *Applied Soft Computing* **51**, 168–179 (2017).
46. Shi, H. & Lv, F. A blind digital watermark technique for color image based on integer wavelet transform. In *2010 International Conference on Biomedical Engineering and Computer Science*, 1–4 (IEEE, 2010).
47. Makbol, N. M. & Khoo, B. E. A hybrid robust image watermarking scheme using integer wavelet transform, singular value decomposition and arnold transform. In *Advances in Visual Informatics: Third International Visual Informatics Conference, IVIC 2013, Selangor, Malaysia, November 13-15, 2013. Proceedings 3*, 36–47 (Springer, 2013).
48. Ling, H.-C., Phan, R.C.-W. & Heng, S.-H. Comment on "robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition". *AEU - International Journal of Electronics and Communications* **67**, 894–897. https://doi.org/10.1016/j.aeue.2013.04.013 (2013).
49. Su, Q., Niu, Y., Liu, X. & Zhu, Y. A blind dual color images watermarking based on iwt and state coding. *Optics Communications* **285**, 1717–1724 (2012).
50. Alawida, M., Samsudin, A. & Teh, J. S. Enhancing unimodal digital chaotic maps through hybridisation. *Nonlinear Dynamics* **96**, 601–613 (2019).
51. Alshoura, W. H., Zainol, Z., Teh, J. S. & Alawida, M. A new chaotic image watermarking scheme based on svd and iwt. *IEEE Access* **8**, 43391–43406. https://doi.org/10.1109/ACCESS.2020.2978186 (2020).
52. Alawida, M. A novel chaos-based permutation for image encryption. *Journal of King Saud University - Computer and Information Sciences* **35**, 101595. https://doi.org/10.1016/j.jksuci.2023.101595 (2023).

53. Singh, A. K., Dave, M. & Mohan, A. Hybrid technique for robust and imperceptible image watermarking in dwt-dct-svd domain. *National Academy Science Letters* **37**, 351–358 (2014).
54. Wu, X. & Sun, W. Robust copyright protection scheme for digital images using overlapping dct and svd. *Applied Soft Computing* **13**, 1170–1182 (2013).
55. Rawat, S. & Raman, B. A blind watermarking algorithm based on fractional fourier transform and visual cryptography. *Signal Processing* **92**, 1480–1491 (2012).
56. Rani, A. & Raman, B. An image copyright protection scheme by encrypting secret data with the host image. *Multimedia Tools and Applications* **75**, 1027–1042 (2016).
57. Fan, T.-Y., Chao, H.-C. & Chieu, B.-C. Medical image watermarking based on visual secret sharing and cellular automata transform for copyright protection. *KSII Transactions on Internet & Information Systems* **12** (2018).
58. Weber, A. G. The usc-sipi image database: Version 5. http://sipi.usc.edu/database/ (2006).
59. Lai, C.-C. A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm. *Digital Signal Processing* **21**, 522–527 (2011).
60. Makbol, N. M. & Khoo, B. E. Robust blind image watermarking scheme based on redundant discrete wavelet transform and singular value decomposition. *AEU-International Journal of Electronics and Communications* **67**, 102–112 (2013).
61. Khan, M. I., Rahman, M., Sarker, M., Hasan, I. *et al.* Digital watermarking for image authenticationbased on combined dct, dwt and svd transformation. arXiv preprint arXiv:1307.6328 (2013).
62. Harish, N., Kumar, B. & Kusagur, A. Hybrid robust watermarking techniques based on dwt, dct, and svd. *International Journal of Advanced Electrical and electronics engineering* **2**, 137–143 (2013).
63. Thakur, S., Singh, A. K., Ghrera, S. P. & Elhoseny, M. Multi-layer security of medical data through watermarking and chaotic encryption for tele-health applications. *Multimedia tools and Applications* **78**, 3457–3470 (2019).
64. Ansari, I. A., Pant, M. & Ahn, C. W. Robust and false positive free watermarking in iwt domain using svd and abc. *Engineering Applications of Artificial Intelligence* **49**, 114–125 (2016).
65. Kumar, S., Sharma, N. K. & Kumar, N. Wsomark: An adaptive dual-purpose color image watermarking using white shark optimizer and levenberg-marquardt bpnn. *Expert Systems with Applications* **226**, 120137. https://doi.org/10.1016/j.eswa.2023.120137 (2023).
66. Lagzian, S., Soryani, M. & Fathy, M. Robust watermarking scheme based on rdwt-svd: Embedding data in all subbands. In *2011 International Symposium on Artificial Intelligence and Signal Processing (AISP)*, 48–52 (IEEE, 2011).
67. Loukhaoukha, K. Image watermarking algorithm based on multiobjective ant colony optimization and singular value decomposition in wavelet domain. *Journal of Optimization* **2013** (2013).
68. Ali, M. & Ahn, C. W. An optimized watermarking technique based on self-adaptive de in dwt-svd transform domain. *Signal Processing* **94**, 545–556 (2014).
69. Teoh, Y. J., Ling, H.-C., Wong, W. K. & Basuki, T. A. A hybrid svd-based image watermarking scheme utilizing both u and v orthogonal vectors for robustness and imperceptibility. *IEEE Access* **11**, 51018–51031. https://doi.org/10.1109/ACCESS.2023.3279028 (2023).
70. Ernawan, F. & Kabir, M. N. A block-based rdwt-svd image watermarking method using human visual system characteristics. *The visual computer* **36**, 19–37 (2020).
71. Ahmadi, S. B. B., Zhang, G., Wei, S. & Boukela, L. An intelligent and blind image watermarking scheme based on hybrid svd transforms using human visual system characteristics. *The Visual Computer* **37**, 385–409 (2021).
72. Gul, E. & Toprak, A. N. Contourlet and discrete cosine transform based quality guaranteed robust image watermarking method using artificial bee colony algorithm. *Expert Systems with Applications* **212**, 118730. https://doi.org/10.1016/j.eswa.2022.118730 (2023).
73. Ahmadi, S. B. B., Zhang, G., Rabbani, M., Boukela, L. & Jelodar, H. An intelligent and blind dual color image watermarking for authentication and copyright protection. *Applied Intelligence* **51**, 1573–7497. https://doi.org/10.1016/j.eswa.2023.120137 (2021).

Acknowledgements

This work was fully supported by Abu Dhabi University under Grant No. 19300887. The author expresses gratitude to the Office of Research & Sponsored Programs at Abu Dhabi University in the United Arab Emirates for their support of this research article.

Author contributions

Wafa' Hamdan Alshoura: Conceptualization, Methodology, Software preparation, Coding, Visualization, Writing - original draft, Data curation, Experimentation. Moatsum Alawida: Conceptualization, Visualization, Methodology, Supervision, Formal analysis, Validation, Reviewing, and Editing.

Declarations

Competing interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Additional information

Correspondence and requests for materials should be addressed to M.A.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.