INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE

ISSN: 2057-5688

Secure and robust digital image watermarking scheme using logistic and RSA encryption

Addagatla Sagar(158r1a0404), Aleti Mounika(158r1a0408), Anisha Kumari Jha(158r1a0412), Ankam Yashashwini(158r1a0413)
Department Of ECE, CMR Engineering College,Hyderabad, Telangana, India,

Abstract : In the era of big data and networking, it is necessary to develop a secure and robust digital watermarking scheme with high computational efficiency to protect copyrights of digital works. However, most of the existing methods focus on robustness and embedding capacity, losing sight of security or requiring significant computational resources in the encryption process. This paper proposed a new digital image watermarking model based on scrambling algorithm Logistic and RSA asymmetric encryption algorithm to guarantee the security of the hidden data at the foundation of large embedding capacity, good robustness and high computational efficiency. The experiments involved applying the encryption algorithms of Logistic and RSA to the watermark image and performing the hybrid decomposition of Discrete wavelet transform (DWT) and Singular Value Decomposition (SVD) on the host image, and the watermark was embedded into the low-frequency sub-band of the host. The values of PSNR and NCC were measured to estimate the imperceptibility and robustness of the proposed watermarking scheme, and the CPU running time was recorded to measure the complexity of the proposed main algorithm in execution time.Experimental results showed the superiority of the proposed watermarking scheme.

Keywords: Image watermarking, DWT, SVD, Logistic, RSA.

I. Introduction :

In the era of rapid development of digitalization and network technology, information sharing becomes much easier. A noteworthy fact is that, multimedia objects stored in the digital format are subject to cyber attacks in an unsecure public channel. First of all, digital media can be easily copied and re-disseminated by a cybercitizen when spreading in a public channel. The process costs low and the information is transmitted with no degradation, but it is unlikely to guarantee that the behavior is legitimate. In addition, digitalized media are easily manipulated by the use of computers. For example, one cracker could selectively crop and integrate part of a digital work into her or his own one, ignoring the copyright of the original work. It is

ISSN: 2057-5688

obviously to see that encryption is an applicable way to make digital media secure. However, if the data is decrypted viciously into its original form, it will put in danger once again. Taking the above analysis into consideration, some researchers have found that digital watermarking technology can solve the security problem to a certain degree. The basic idea of this kind of technology is to use copyright information, data block header information or time synchronization mark data as watermark information, and embed them into a host signal, such as image, audio, or video and the likes. In this way, the watermark information is not transmitted in another digital channel, but transmitted as part of the host signal. Apart from protecting copyright of digital works, a qualified watermarking system requires that the process of embedding some extra data should bring the least degradation to the host signal, which means that the host data should not be changed visually after inserting the watermark information. Moreover, the watermarking system needs to be robust against possible cyber attacks. The extra data should not be removed or changed after the watermark information experiences a certain attack in a network environment. But if the host object is changed, the watermark data will be lost.

Digital watermarking is generally divided into spatial domain watermarking and frequency domain watermarking. Depending on the embedding domain chosen, the degree of robustness and invisibility of systems, the data embedding capacity has an effect on the robustness and imperceptibility of watermark (Verma & Jha, 2015). Usually, embedding data in frequency domain works better than that in spatial domain for the better robustness to resist multiple signal processing manipulations and attacks. In order to solve the ambiguous problem of watermark, YAVUZ and TELATAR (2007) applied three-dimensional discrete wavelet transform (DWT) to a host image, and four sub-bands of low-low (LL), high-low (HL), low-high (LH) and high-high (HH) were obtained. The watermark was image was decomposed by singular had the value decomposition (SVD). The singular values (SV) of watermark was then embedded into that of the sub-bands LL and HL from host image, and left singular matrix (U) of the watermark image was embedded into LH and HH of the host image. Mukherjee and Pal (2012) got discrete cosine transform (DCT) coefficients from the process of DCT transform of host image, and formed a new host image. The watermark was embedded into the new image by the course of SVD decomposition and recombination. Wang, Li and Kang (2015)

ISSN: 2057-5688

divided host image into sub-blocks of
m n , and performed DCT transform on each block. The watermark was then condensed and embedded into the intermediate frequency coefficients of the host image together with the decoded secret key. For the sake of security of digital watermark, watermark can be scrambled, and the Arnold's method is widely used. Sujatha and Sathik (2010) obtained the minimum values from each sub-block of the host image, scrambled those values three times with Arnold transform, and constructed a binary watermark. After DWT performed on the host image, watermark information is embedded into high frequency coefficients of the host. The sub-blocks of host image was processed by DCT and further quantized in (Han, Yang, Zhi, 2011). The watermark image was then embedded in the selected DC coefficients after scrambled by Arnold procedure. Prasad (2013) extracted parts of data from the spatial domain of the host image as a digital watermark, and employed one level DWT on the host image. Watermark was scrambled by Arnold and embedded in high frequency sub-band of the host image. Saikrishna and Resmipriya (2016) separated host image into two texture regions of white and black, decomposed them with two levels of DWT, and scrambled watermark with Arnold. The scrambled data was embedded in sub-bans of the white textured area. Niu, Cui, Li and Ding (2016) decomposed hostimage with two level DWT (2-DWT) and applied SVD to the sub-bands of low frequency of the host and the scrambled watermark, and got the watermarked image by use of adding their singular values. Sikder, Dhar and Shimamura (2017) proposed a novel watermarking technique in which a host image was performed by slant transform and lower upper decomposition successively. The extra data were encrypted by Arnold function and then inserted into the obtained upper triangular matrix to resist some common image attacks. Those works above can reach robustness to a certain degree and maintain the visual quality of watermarked image. But the transformation cycle of Arnold is not long, if attackers carried out a limited times of scrambling process continuously, they could restore the original image. That is, Arnold has a low degree of security for its small size of secret key space. To achieve a higher level security, the works in (Kishore, Venkatram, Sarvya, & Reddy, 2014; Saha, Pradhan, Kabi, & Bisoi, 2014; Ray, Padhihary, Patra, & Mohanty, 2015; Patel, P. & Patel, Y., 2015) all encrypted the watermark image with RSA data encryption algorithm, which raises a new issue that image encryption with RSA is time consuming.

Some researchers have made use of

ISSN: 2057-5688

technique of joint fingerprinting and decryption (JFD) to save the computational time. Kundur and Karthik (2004) used JFD for media encryption and fingerprinting in the area of digital rights management. The fingerprinting process was done on the receiver side, thus the media was encrypted once before being sent to users to achieve the purpose of saving the computational time. Similarly, in the method proposed by Czaplewski and Rykaczewski (2014), the host image was encrypted by a matrix multiplication based block cipher algorithm, and the encrypted image was then transmitted to different uses. After decrypting the received image, the process of fingerprint embedding was conducted on the coefficients of discrete cosine transform domain. Czaplewski (2016)used the method of quaternion algebra to rotate and translate the components of the host image in a three-dimensional color space, and encrypted the image at the source. Receivers designed different decryption keys according to their own fingerprints, and inserted the fingerprints into the image decrypted. The advantage of the JFD algorithm is that the watermark embedding process is placed at the receiving end, without considering the robustness of the watermark subject to various attacks when transmitted on the network, resulting in less time consumption on the receiving side. However, the data embedding capacity is limited in those algorithms, and their security needs to be improved. They utilise difference information entropy between encryption keys and decryption keys to form digital fingerprints, leading to a situation that a large amount of difference information will cause serious distortion to the host image. Thus, the embedded fingerprint is relatively small. In addition, the technique of symmetric encryption is applied in their algorithms although the keys used in encryption and decryption are different, and the distributor must know each user's decryption key to complete the process of copyright authentication. So the security risk arises when processing secret key management and distribution.

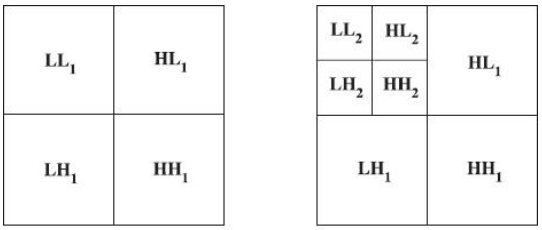
To address the above mentioned issues, we attempted to lower the consuming time as well as to improve the security of watermark apart from ensuring high robustness. Subsequently we proposed a new image watermarking scheme based on DWT, SVD, Logistic and RSA. The rest of this paper is organized as follows. In section 2, we discuss the principle of DWT, SVD, Logistic and RSA. In section 3, we propose our new watermarking scheme including embedding and extraction process. In section 4, experimental results and discussion are presented. In section 5, we briefly conclude what we contribute

INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688

II. Preliminaries

Discrete wavelet transform

Discrete wavelet transform (DWT) is a process of multi-scale and spatial-frequency decomposition to an image. In the DWT-based watermarking scheme, DWT is used to decompose an aimed image into four types of sub-bands which are LL, HL, LH and HH. LL is low frequency component,



(a) (b)

and has a low resolution, representing approximate information of an image. The other three are horizontal high-frequency part, vertical high-frequency part, and high frequency part, respectively, and their resolutions are high, representing detailed image information. One or more sub-bands can be used to embed watermark information. DWT is an efficient frequency model for HVS, which is widely applied in the field of image compression and enhancement. Wavelet transform has the characteristics of multi-resolution, so hierarchical display is a feasible application of continuous image transmission. In watermark applications, it has less computation complexity when watermark is embedded hierarchically or nested by using DWT technology

DWT-based techniques reflect better robustness against various attacks comparedwith watermarking in spatial domain (Verma & Jha, 2015). Another feature of DWT is the ability to select different filter banks for the required broadband. The commonly used filters are Haar, Daubechies, Coiflets and Biorthogonal, and adjustments can be easily done when necessary. With regard to a multidimensional signal, the ideal of DWT is to split the signal into high and low frequencies, and the low frequency part is further split up into high and low frequencies until the original signal is completely decomposed, as shown in Figure 1. After the process of inverse wavelet transform (IDWT), the image can be reconstructed and restore from the DWT coefficients.

Figure 1 (a) 1-level DWT, (b) 2-level DWT

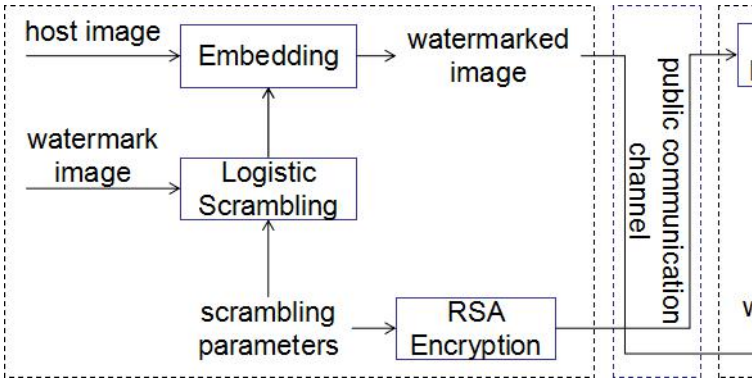
Singular Value Decomposition

Singular Value Decomposition (SVD) is commonly used in linear algebra (Verma & Jha, 2015). This mathematical tool can be used in many applications, such as signal or image processing, including digital watermarking. In a SVD-based watermarking technique, SVD usually acts on the host image, or the host image is first divided into many small blocks and then those blocks are decomposed with SVD

INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688

III. The Proposed Algorithm

In this section, we present a new watermarking scheme in Figure 2, which contains two main processes of watermark embedding and watermark extraction. Watermark preprocessing and embedding procedure are performed on the sending side, and the watermarked image is transmitted to the receiver over the internet. At the receiving end, watermark extraction and recovery is carried out. The blocks in the figure represent the corresponding algorithm operations. Arrow symbols pointing to them means that some words nearby are the inputs of the operation. The main processes of our proposed scheme are that watermark was first scrambled by Logistic, and the scrambling parameters were encrypted by RSA and then transmitted through network. In the process of watermarking embedding, one level discrete wavelet transform was applied to the host image and a low-frequency sub-band was then obtained. The sub-band was further processed by Singular value decomposition. Plus singular value of the sub-band and the scrambled watermark, and new singular value was acquired. In the addition operation, a scaling factor was chosen to control the embedding strength of watermark, and an appropriate strength could be traded off between imperceptibility and robustness. This new value was decomposed once again to get a new singular value which was used to reconstruct a low-frequency sub-band. Finally, the watermarked image was formed by making using of the new sub-band after the process of inverse discrete wavelet transform. The details of watermark embedding and extraction are depicted in Sections 3.1 and 3.2



a. Watermark Embedding

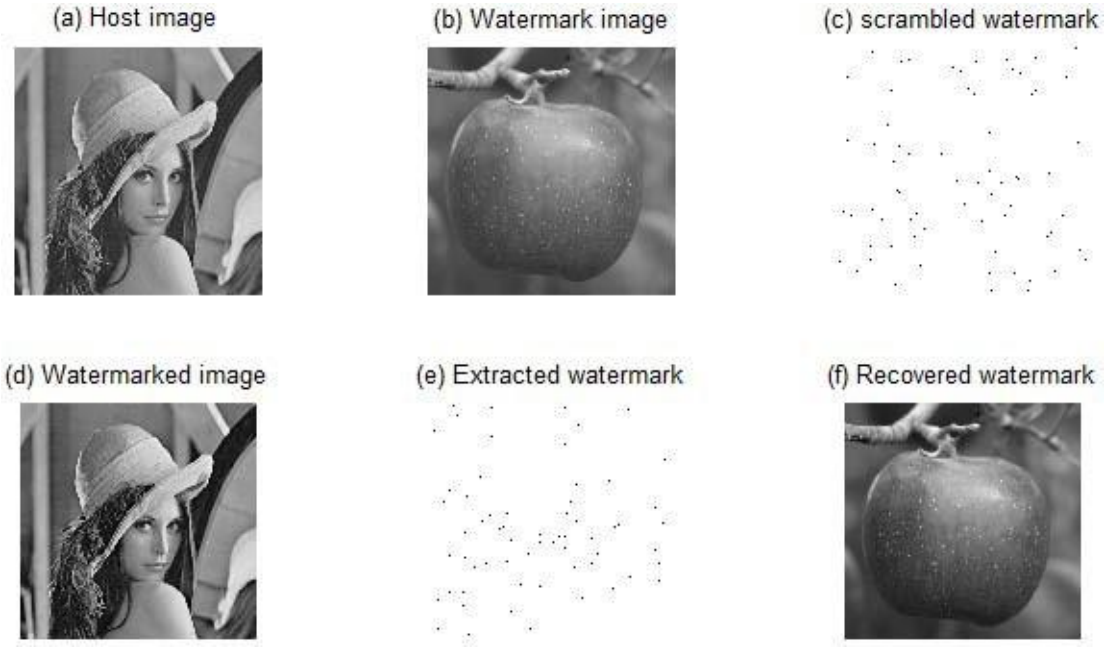
In the procedure of watermark embedding, a watermark image was first scrambled by using a Logistic algorithm before being embedded into the transformed domain of the host image. Assuming that the pixel information of watermark can be denoted as m-by-m matrix A, A is reshaped to a 1-by-m*m matrix T, whose elements are taken column-wise from A. $x(i)$ is a one-dimension array with a length of m^2, and given a initial $x(0)$ and a system parameter u, a chaotic sequence is generated in the process of iteratively calculating $x(0)$ and u by the formula given in Section 2.3, and elements of the sequence is saved in $x(i)$ successively. The array is then normalized to become a new sequence in range of (0, 255) through the following formula:

IV. Experimental results and discussion

A series of experiments were conducted to validate the

ISSN: 2057-5688

effectiveness of the proposed scheme with the method proposed



watermarking scheme, which was further compared with the related methods. Table 1 shows the CUP running time in the process of watermark encryption using Saha, Pradhan, Kabi and Bisoi (2014)'s scheme, Kishore, Venkatram, Sarvya and Reddy (2014)'s scheme, and our proposed scheme. Saha et al.'s scheme represents a class of algorithms that use the asymmetric encryption algorithm RSA for the watermark image. They yielded higher security compared with the methods based on symmetric key encryption. However, encrypting the image with RSA consumes more time, which is confirmed later in our experiments. Figures 3-5 and Table 2 are the results of the proposed scheme with a scaling factor of 0.005, and Table 3 is the result with the factor of 0.05. Table 3 compares NCC values between the proposed by Kishore, Venkatram, Sarvya and Reddy (2014) and the method proposed by Saha, Pradhan, Kabi and Bisoi (2014) in case of various types of attacks. Kishore et al.'s method is a typical frequency domain watermarking algorithm that embeds watermark into low-frequency sub-band after applying DWTto the host image, but the use of hybrid decomposition can make up for some of its flaws.

Figure 3(f), the details of this proposed watermarking scheme are depicted. Figure 3(c) shows the scrambled watermark with the scrambling parameters of 0.2 and 3.6. Figure 3(d) shows the watermarked image based on the combination of one level discrete wavelet transform and singular value

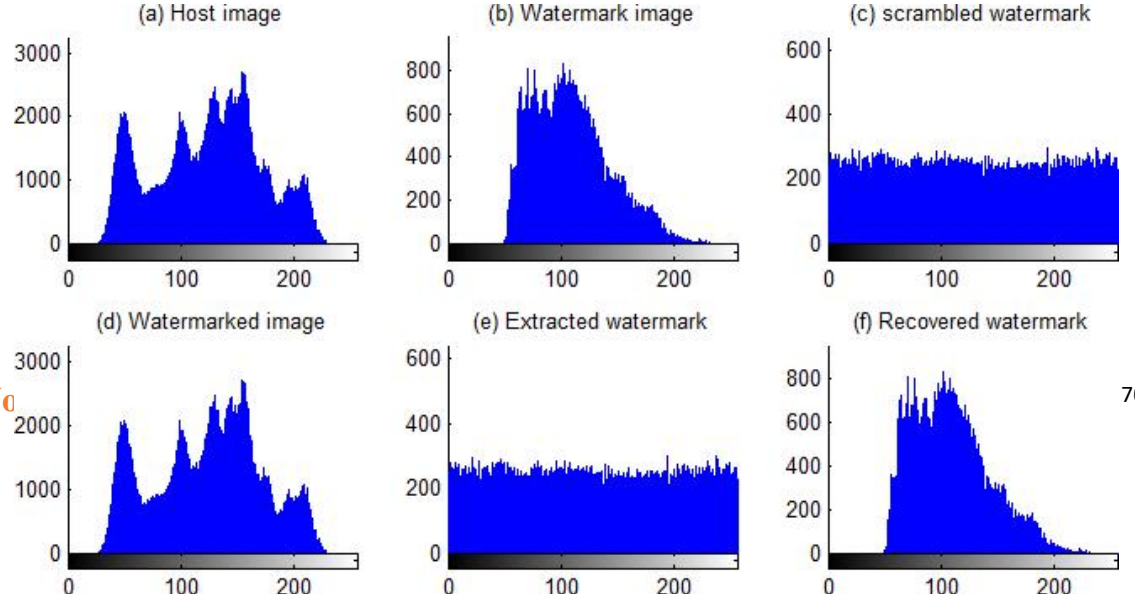
ISSN: 2057-5688

decomposition and the scaling factor was 0.005. Figure 3(e) shows the extracted watermark from the watermarked image, and the extracted image is in a chaotic state. Figure 3(f) shows the watermark recovered from the extracted image with the same scrambling parameters.

Figures 4(a), (b), (c), (d), (e), and (f) are the histograms of the original host image, watermark image, scrambled watermark, watermarked image, extracted watermark image, and recovered watermark, respectively. These histograms reflect the pixel distribution of corresponding images, where the horizontal axis represents different level grayscales of an image, and the vertical axis the number of pixels of a certain grayscale. Normally, if an image is changed, its pixel distribution will change, too. Taking Figure 4(a) as an example, the composition of histogram of the host covered a wide range of gray levels as a result of the high contrast of the host image. The results of Figs. 4(a) and (d) indicated a small impact on the host image from the extra data, indicating the imperceptibility of the proposed scheme. Figs. 4 (c) and (e) show that the watermark image was scrambled with a high degree, and Figs. 4 (b) and (f) show a high similarity between the original watermark and the recovered watermark image.

Figure 4. Hist of (a) host image, (b) watermark image, (c) scrambled watermark, (d) watermarked image, (e) extracted watermark, and (f) recovered watermark

Table 1 compares the elapsed time in RSA encryption and decryption of the proposed scheme and scheme of Saha, Pradhan, Kabi and Bisoi (2014) and Kishore, Venkatram, Sarvya and Reddy (2014). The prime numbers of p and q were randomly chosen for calculating n, one of secret keys. Three sets of numbers of this kind were taken to test the CUP running time. As shown in Table 1, the encryption and decryption processes using Saha et al and Kishore et al.'s methods need more time than the proposed scheme. As the volume of encrypted object increases, the time required for RSA encryption increases, too. A watermark image is



ISSN: 2057-5688

a data matrix, and it takes time to encrypt it. The proposed scheme first scrambles the watermark and then encrypts the scrambling parameters with RSA. Scrambling parameters can be regarded as a string of several characters. So the proposed scheme is less time-consuming. proposed scheme outperforms the methods proposed by Saikrishna et al. (2016) and Han et al. (2011) in terms of the robustness of watermark. Taking cropping attacks as an example, we averagely disseminated the watermark information into the cover image, so the cropping part of image did not degrade the quality of the embedded datanoticeably.

Table 6. Comparisons in NCC values

Manipulations	Our method	Saikrishna and Resmipriya (2016)	Han, Yang and Zhi (2011)
Mean Filtering (3×3)	**0.7574**	0.7348	0.6947
Mean Filtering (5×5)	0.6053	**0.6513**	**0.6372**
Median Filtering (3×3)	0.9517	**0.9682**	0.9274
Median Filtering (5×5)	**0.8628**	0.8607	0.7849
Rotation (15)	**0.8649**	0.8573	0.8618
Rotation (30)	**0.7529**	0.6947	0.7158
Rotation (45)	**0.7629**	0.7121	0.6895
Gaussian Noise (0.001)	**0.9437**	0.9429	0.8978
Gaussian Noise (0.005)	0.9029	**0.9173**	0.8436
Gaussian Noise (0.01)	**0.8546**	0.8176	0.7648
Salt & Pepper Noise (0.05)	0.9237	**0.9461**	**0.9341**
Salt & Pepper Noise (0.1)	**0.8521**	0.8273	0.8312

ISSN: 2057-5688

Salt & Pepper Noise (0.3)	**0.7875**	0.7648	0.7719
Salt & Pepper Noise (0.5)	**0.6792**	0.6486	0.6651
Crop (50,50)	**0.9673**	0.9347	0.9543
Crop (100,100)	**0.9567**	0.9138	0.8952
Crop (150,150)	**0.9276**	0.8750	0.8217
Crop (200,200)	**0.8657**	0.8139	0.6976
JPEG (40%)	0.6292	**0.6471**	0.6127
JPEG (30%)	0.8015	0.7938	**0.8146**
JPEG (20%)	**0.8738**	0.8673	0.8706
JPEG (10%)	0.9217	**0.9341**	**0.9357**

To quantify the watermarking property and to prove the advantage of less time consumption in the proposed scheme, an experiment was implemented on the platform of MATLAB 7.0 running on a PC with a CPU of Inter Core2 2.66 GHz and a memory chip of 4 GB. From the visual effects of Figure 3 and statistic data of Figure 4, it is noted that the proposed watermarking algorithm had a good imperceptibility. Table 2 and Figure 5 show the results for watermarked images and recovered watermark after various attack tests with a low embedding intensity and the mean NCC value was 0.8325, indicating a good visibility in the extracted watermark. When the intensity was increased to 0.05, as shown in Table 3, most NCC values of the proposed scheme were bigger than those of Kishore, Venkatram, Sarvya and Reddy (2014)'s scheme, and the mean NCC value was improved to 0.8566, illustrating that the proposed watermarking algorithm had good robustness. Apart from considering the properties of robustness and imperceptibility, the proposed scheme also focus on security and computational complexity. While preserving the security of RSA, we attempted to reduce the time consumed by the scheme as much as possible, and have made several improvements. The comparisons as shown in Table 1 indicated that the proposed encryption process cost less time than Saha, Pradhan, Kabi, and Bisoi (2014)'s scheme, for the reason that the watermark image was

ISSN: 2057-5688

directly encrypted by RSA encryption algorithm in the latter scheme but this process required a longer time to proceed, while the former scheme (proposed) was first to encrypt watermark with a Logistic algorithm that needs less time and then to encrypt the encryption parameters of Logistic with RSA, which not only guaranteed security of watermark but also reduced the time elapsed.

V. Conclusion

In this paper, an improved secure and robust digital watermarking scheme has been proposed. The embedding process includes embedding a gray-scale image into the singular value of low frequency sub-band of the host image. The combination of a image-scrambling algorithm and a secure data-encryption algorithm was used to improve the security of the proposed watermarking scheme. The scrambling parameters could be stolen when information is transformed on a public network, but the asymmetric encryption system can protect those parameters form being attacked by hackers. The simulation experiments demonstrated that the proposed scheme had taken the main performance of watermarking technique into consideration and outperformed other similar approaches, having better robustness, less encryption time
and large data embedding capacity. In the era of big data, a huge amount of digital images need to be processed and then transmitted through the network full of various threats. The issues of computational refinement and data security attract more and more people's attention and the proposed scheme addresses these two points to some extent. In the future, guaranteeing the data security of image watermarking is an important direction and the use of asymmetric encryption method should be a good choice.

VI. References

[1] H. Tao, L. Chongmin, J. M, Zain, and A. N. Abdalla, ''Robust image watermarking theories and techniques: A review,'' J. Appl. Res. Technol., vol. 12, no. 1, pp. 122–138, Feb. 2014.

[2] S. Voloshynovskiy, S. Pereira, T. Pun, J. J. Eggers, and J. K. Su, ''Attacks on digital watermarks: Classification, estimation based attacks, and benchmarks,'' IEEE Commun. Mag., vol. 39, no. 8, pp. 118–126, Aug. 2001.

[3] H. Nyeem, W. Boles, and C. Boyd, ''Digital image watermarking: Its formal model, fundamental properties and possible attacks,'' EURASIP J. Adv. Signal Process., vol. 2014, p. 135, Dec. 2014.

[4] N. Zivic, ''Watermarking for Image Authentication,'' in Robust Image Authentication Presence Noise, 1st ed. Cham, Switzerland: Springer, 2015, pp. 43–47.

ISSN: 2057-5688

[Online]. Available: http://www.springer.com/in/book/9783319131559

[5] S. A. Parah, F. Ahad, J. A. Sheikh, and G. M. Bhat, ''Hiding clinical information in medical images: A new high capacity and reversible data hiding technique,'' J. Biomed. Inf., vol. 66, pp. 214–230, Feb. 2017, doi: http://doi.org/10.1016/j.jbi.2017.01.006.

[6] S. A. Parah, F. Ahad, J. A. Sheikh, and G. M. Bhat, ''A new reversible and high capacity data hiding technique for E-healthcare applications,'' Multimed Tools Appl., vol. 76, no. 3, pp. 3943–3975, Feb. 2017.

[7] S. A. Parah, J. A. Sheikh, J. A. Akhoon, N. A. Loan, and G. M. Bhat, ''Information hiding in edges: A high capacity information hiding technique using hybrid edge detection,'' Multimed Tools Appl., vol. 77, no. 1, pp. 185–207, 2018, doi: 10.1007/s11042-016-4253-x.

[8] S. A. Parah, F. Ahad, J. A. Sheikh, N. A. Loan, and G. M. Bhat, ''Information hiding in medical images: A robust medical image water marking system for E-healthcare,'' Multimed Tools Appl., vol. 76, no. 8, pp. 10599–10633, Apr. 2017.

[9] R. Eswaraiah and E. S. Reddy, ''Robust medical image watermarking technique for accurate detection of tampers inside region of interest and recovering original region of interest,'' IET Image Process., vol. 9, no. 8, pp. 615–625, 2015.

[10] M. Benyoussef, S. Mabtoul, M. E. Marraki, and D. Aboutajdine, ''Robust ROI watermarking scheme based on visual cryptography: Application on mammograms,'' J. Inf. Process. Syst., vol. 11, no. 4, pp. 495–508, Dec. 2015.

[11] L. Gao, T. Gao, G. Sheng, and S. Zhang, ''Robust medical image watermarking scheme with rotation correction,'' in Intelligent Data analysis and its Applications. Cham, Switzerland: Springer, 2015, pp. 283–292.

[12] K. Muhammad, J. Ahmad, S. Rho, and S. W. Baik, ''Image steganography for authenticity of visual contents in social networks,'' Multimedia Tools Appl., vol. 76, no. 18, pp. 18985–19004, 2017. [Online]. Available: https://doi.org/10.1007/s11042-017-4420-8

[13] A. Kanso and M. Ghebleh, ''An efficient and robust image encryption scheme for medical applications,'' Commun. Nonlinear Sci. Numer. Simulat., vol. 24, nos. 1–3, pp. 98–116, Jul. 2015.

[14] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. W. Baik, ''A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image,'' Multimedia Tools Appl., vol. 75, no. 22, pp. 14867–14893, 2016.

[15] M. M. Abd-Eldayem, ''A proposed security technique based on watermarking and encryption for digital imaging and communications in medicine,'' Egyptian Informat. J., vol. 14, no. 1, pp. 1–13, Mar. 2013.

[16] J. B. Lima, F. Madeiro, and F. J. R. Sales, ''Encryption of medical images based on the cosine number transform,'' Signal Process., Image Commun., vol. 35, pp. 1–8, Jul. 2015.

ISSN: 2057-5688

[17] B. Li, J. He, J. Huang, and Y. Q. Shi, ‘‘A survey on image steganography and steganalysis,’’ J. Inf. Hiding Multimedia Signal Process., vol. 2, no. 2, pp. 142–172, 2011.

[18] W. Luo, F. Huang, and J. Huang, ‘‘Edge adaptive image steganography based on LSB matching revisited,’’ IEEE Trans. Inf. Forensics Security, vol. 5, no. 2, pp. 201–214, Jun. 2010.

[19] K. Muhammad, J. Ahmad, N. U. Rehman, Z. Jan, and M. Sajjad, ‘‘CISSKA-LSB: Color image steganography using stego key-directed adaptive LSB substitution method,’’ Multimedia Tools Appl., vol. 76, no. 6, pp. 8597–8626, 2017.

[20] K. Muhammad, M. Sajjad, I. Mehmood, S. Rho, and S. W. Baik, ‘‘Image steganography using uncorrelated color space and its application for security of visual contents in online social networks,’’ Future Generat. Comput. Syst., vol. 2, Nov. 2016. [Online]. Available: https://doi.org/10.1016/j.future.2016.11.029

INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688