Robust and Secure Watermarking for Propagation of Digital Multimedia by Paillier Homomorphic Cryptosystem With Arnold Transformation

Namita Agarwal, Jaypee University of Information Technology, India

Pradeep Kumar Singh and http, Jaypee University of Information Technology, India

ABSTRACT

Sharing of digital media over internet is becoming easier due to content authentication and security provided by digital watermarking. It also locates application in other fields like copyright protection, tele-medicine, military, tamper detection, and many more. This paper represents the robust watermarking approach using Paillier homomorphic cryptosystem with Arnold transformation. In this, the watermarking system is primarily prepared at an encrypted DWT-DCT domain. Cryptosystem is exploited at this time to encrypt the original media. For more security of multimedia content, the watermark image is scrambled through Arnold scrambling technique. The embedding process is done here to produce the encrypted watermark image followed by the encryption process. At recovery phase, decryption of encrypted watermark image to get the original and watermark image is done. The experimental result has shown that watermarking method is more robust and offers the security of digital media.

KEYWORDS

Healthcare Technologies, Information Security, Multimedia Systems, Watermarking

1. INTRODUCTION

Nowadays digital documents are increasing with a terrifying amount, security of these documents by effective techniques are major concern in the field of research from last few decades. So, the digital watermarking is found suitable for copyright protection, owner identification and security etc. Kaur et al. (2020) and Zhang et al. (2016). Watermarking is the method of implanting a single or dual secret information in terms of tag, label or digital signal into an original media Patel et al. (2011). The cover image is embedded with the watermark image in a visible or invisible manner, where secret information is watermark image in Nikolaidis et al. (1998) and Xianghong et al. (2003). There are many research problems in the field of digital watermarking like imperceptibility of watermark, security and robustness which needs to be enhanced in Eyadat et al. (2005) and Liyun et al. (2006). Thus, watermark embed in such a way that quality of original media does not damage and watermark cannot be extracted effortlessly in Liyun et al. (2006) and Xianghong et al. (2003). Further, digital watermarking method can be classified on various categories on the basis of domain, robustness, type of media, recovery process and perceptivity. A simple organization of digital watermarking is shown in fig.1.

According to domain based, watermarking techniques can be divided into two spatial domain or transform domain in Aslantas, (2008) and Loukhaoukha et al. (2014). In spatial domain method embedding can be done by altering the image pixels directly, whereas in transform domain, watermark is embedded by modifying the coefficients of transformed image Rawat et al. (2012) and Su et al. (2013). Spatial domain methods have low computational cost and easy to use rather than transform domain techniques. Least significant bit, spread spectrum and correlation are some common techniques of spread spectrum domain according to Maity et al. (2011). However, transform domain watermarking has discrete cosine transform (DCT), Discrete wavelet transform (DWT), Singular value decomposition (SVD), Quaternion Hadamard Transform (QHT) and many other Santhi et al. (2013). Nowadays researchers are working on watermarking with cryptography for securing the digital media Priya et al. (2018). Modern cryptography follows a strong scientific method and plans cryptographic algorithms, making such algorithms hard to break by an opponent. On the basis of above discussions robust and secure watermarking method for color image using cryptosystem and Arnold transformation is presented. The scheme presented in paper is novel because of following contributions:

1. Here, we present an innovative robust and secure watermarking based on Paillier cryptosystem and Arnold transformation for color image.
2. The requirements of robustness and transparency in digital watermarking approaches are always a trade-off in applications. Robustness of proposed method is increased with better imperceptibility of watermark image.
3. The proposed method is also robust against attacks, such as salt & pepper, filtering, compression and rotation etc.

The remaining work discussed in this manuscript is as literature review used in this paper is described in section 2, preliminaries used in this paper are described in section 3. Proposed algorithm with watermarking process followed by encryption procedure is described in section 4. An analysis section with comparison results is presented in section 5. Finally, the conclusion section is represented in section 6.

2. LITERATURE REVIEW

Some important watermarking methods have been proposed in last years by probable researchers are as follows:

In Horng et al. (2014), for e-governance application an adaptive watermarking scheme is discussed using DCT and SVD. For optimize the gain factor of masking genetic algorithm is also used. this technique offers robust results to many attacks and evade the false positive problem. Author discussed a watermarking method based on wavelet domain in Atawneh et al. (2017). The method is based on DWT and diamond encoding scheme to deliver a high embedding capacity and distortion control watermarking. Using an incarnation of different transform domain techniques i.e. DWT, DCT and SVD author have discussed a robust and imperceptible watermarking scheme in Singh et al. (2014). In Trivedy et al. (2017) author presented a logistic map based fragile watermarking method. Experimental outcome like PSNR and false tamper detection have shown that technique found superior than other existing techniques in Chang et al. (2011) and Hsu et al. (2010). In Li et al. (2018), author presented a colour image watermarking technique based on Quaternion discrete cosine transform (QDCT) and singular value decomposition with encrypted binary computer-generated hologram. The proposed technique is secure as well as robust against many attacks. Su and Chen discussed a reversible watermarking method based on quantization in spatial domain in Su et al. (2018). Author proposed a digital image watermarking system for color images in Vahedi et al. (2017). Before embedding the watermark is distinguished into 16 nonoverlapping sub areas and scrambled by spatiotemporal chaotic

Figure 1. Categorization of digital watermarking
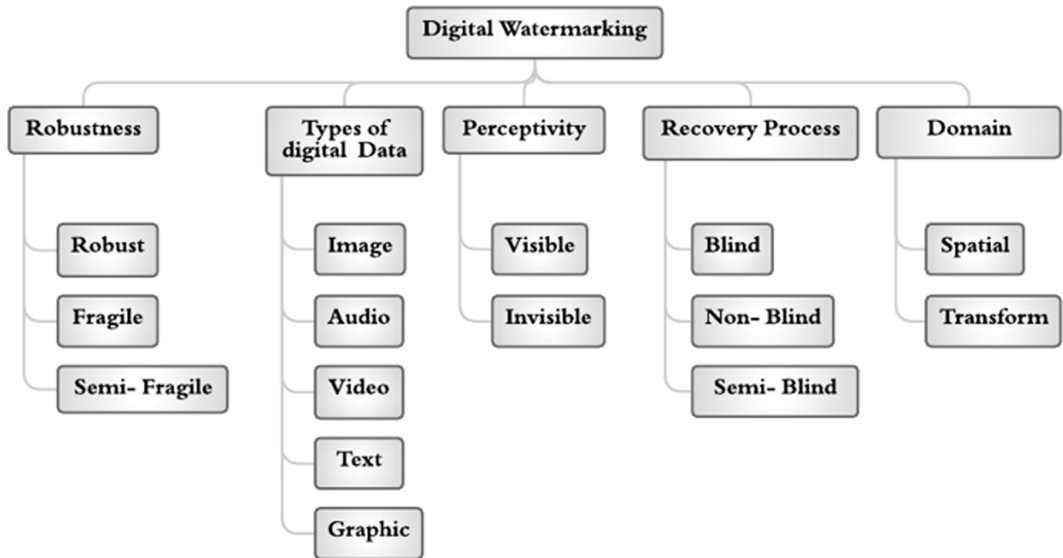
matrices and visual secret sharing matrices. In Liu et al. (2018), they have recently used logistic and RSA encryption for secure and robust image watermarking. They crried out their work as logistic scrambling and RSA encryption for embedding. Analyze results over watermarking in comparison to other schemes and found their method is superior. As their scheme works in DWT- SVD domain, it is found to be robust. But one drawback for this technique is watermark extract in an informed manner. Their scheme requires both the cover and signed images to get extracted watermarks. Boussif et al. (2018) had discussed a proposed secure medical cloud for archiving and transmission of medical data (images and reports). They use AES encryption to encrypt the text file and LSB method for hiding the patient information in the medical image. This technique found superior against different types of attacks. Gupta et al. (2018) inserted a binary watermark in semi-blind approach based on advanced encryption scheme generally known as Elliptic curve cryptography to embed a watermark. The method uses DWT- DVD techniques along with ECC and achieved better results. In Seong et al. (2014), buyer- seller watermarking approach using DCT and homomorphic encryption for image watermarking. They argued that their results have good visibility against image processing attacks. In Jost et al. (2015), have calculated the result of Paillier Cryptosystem. They claim that to deal with the large and growing datasets for processing, encryption recital plays a major role for reasonableness of homomorphic encryption techniques. In this paper they conclude that they have achieve the better performance. In Abdallah et al. (2014) describe the idea of homomorphic image watermarking with SVD. They use homomorphic transform before embedding the chaotically encrypted watermark, then pertain the SVD construction over the reflectance component for the original image. They claim that encryption technique is not used in cover signal. By applying LPF (Low Pass Filtering) and HPF (High Pass Filtering) they implement their watermark embedding in block by block manner. They argued that their block by block manner watermark technique found better results in comparison to full watermarking. They get better results as compared to Liu et al. (2002).

Now, we report detailed Paillier Homomorphic cryptosystem with Arnold scrambling technique is discussed in the next section.

3. PAILLIER HOMOMORPHIC CRYPTOSYSTEM

In 1999, scientist name Pascal Paillier has developed the Paillier encryption method. It is probabilistic public key encryption which has both homomorphic and probabilistic possessions. In homomorphic cryptosystem, without the use of primary decryption, encryption can be done. It can accomplish multiplicative and additive homomorphism. This cryptosystem is combined with DWT and DCT for encryption and decryption of images.

3.1 Steps For Key Generation

1.) Select the two large prime numbers a and b at random but independent to each other such that,

$$\gcd = (ab, (a-1)(b-1)) = 1 \tag{1}$$

2.) Analyze,

$$n = ab, \tag{2}$$

$$\lambda = \frac{\left|(a-1).(b-1)\right|}{\gcd\left(a-1, b-1\right)} \tag{3}$$

where gcd stands for greatest common multiple.

3.) Select the casual number i, where, $i \in \mathbb{Z}_{n^2}^{*}$.
Certify n divides the order of i, by confirming the modular multiplicative inverse that is shown by eq. 4

$$\mu = \left(L\left(i^{\lambda} \bmod n^{2}\right)\right)^{-1} \bmod n \tag{4}$$

Where function L is depicted as

$$L\left(x\right) = \frac{\left(x-1\right)}{n} \tag{5}$$

Encryption
    1.) Take m as a message to be encrypted where $m \in \mathbb{Z}_n$
    2.) Select random integer g, where $g \in \mathbb{Z}_n^{*}$
    Calculate ciphertext:

$$c = i^{m} . g^{n} \bmod n^{2} \tag{6}$$

Decryption

1.) Let's decrypt the ciphertext message c, where $c \in \mathbb{Z}_{n^2}^*$

Calculate the plaintext message as shown in eq. 7:

$$m = L\left(c^{"} \bmod n^2\right). \frac{1}{4} \bmod n \tag{7}$$

3.2 Applying DWT in Encrypted Domain

Wavelet transform has excellent space and energy compaction properties this makes it very important tool in image processing and watermarking. The key idea behind the DWT is that it splits a frequency particular on waves called wavelets of changing frequency for restricted duration by Ali et al. (2018). Each level of decomposition of DWT for analysis of an image divides into four sub-bands on different frequency components at different resolutions. There are two types of sub-bands low pass and high pas. However, Low pas sub bands gives the exact information of original images and information like edges of images can be gained by high pass sub bands. The four sub-bands of 2D DWT are described below:

- Coefficient of Diagonal (cD) is high frequency component in horizontal and vertical (HH) sub-band
- Coefficient of Vertical (cV) is high frequency component in horizontal and low frequency component in vertical (HL) sub-band
- Coefficient of Horizontal (cH) is low frequency component in horizontal and high frequency component in vertical (LH) sub-band
- Coefficient of Approximation (cA) is low frequency component in both horizontal and vertical (LL) sub-band

3.3 Applying DCT in Encrypted Domain

The most substantial data of an image is focused in a low frequency coefficient of the DCT. In case of DCT lower frequency constants are more concentrated rather than high frequency, they may not be focused. DCT can be used in spatial and transform domain watermarking due to its energy compaction properties in Lin et al. (2010). Thus, the 2D DCT transform can be described in eq. 8,

$$F(m, n) = c(m)\, c\,(n) \frac{2}{N} \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f\left(x, y\right) \cos \frac{\left(2x+1\right)m\pi}{2N} \cos \frac{\left(2y+1\right)n\pi}{2N} \tag{8}$$

Where x, y, m, n = 0, 1, 2……, N-1, and

$$c\,(m) = \begin{cases} \dfrac{1}{\sqrt{2}} & for \in = 0 \\ 1 & Otherwise \end{cases} \tag{9}$$

the equation of inverse transform (IDCT) is given below in eq. 10

$$f(x,\,y) = \frac{2}{N} \sum_{m=0}^{N-1} \sum_{n=0}^{N-1} c(m)\, c(n)\, F(m,n)\, \cos\frac{(2x+1)m\pi}{2N}\,\cos\frac{(2y+1)n\pi}{2N} \tag{10}$$

3.4 Arnold Transformation

To increase the security of watermarking process watermark image is randomized before embedding into host image. There are many scrambling techniques but here we choose Arnold transform, it is an iterative process to alter the coordinates of pixel position to change the layout of an image in Singh et al. (2017) and Zhang et al. (2016). According to Agradriya et al. (2019) it has a periodic property that means after several iteration inserted image can get back to the original state. This property can be used as secret keys. Equation 11 shows the 2D Arnold transformation for image is described as:

$$\begin{bmatrix} x_k \\ y_k \end{bmatrix} = \left\{ \begin{bmatrix} 1 & m \\ n & mn+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (mod\,N) \right\}^K \tag{11}$$

Where x_k and y_k are transform pixels consequent to coordinates x and y after K iterations. N represents the height and width of square image treated, m and n are two positive integers.

4. PROPOSED ALGORITHM

The designed method is applicable for watermarking system in an encrypted domain for enhancing the robustness of the multimedia content. In this system the A is encrypted using paillier homomorphic encryption in hybrid domain DWT-DCT and get encrypted image E[A]. After that secret image is scrambled using Arnold transformation for producing the scrambled image E[W]. It is very difficult to retrieve secret image for unauthorized person after recover phase or extraction. The encrypted cover image and scrambled watermark image are embedded together to get an encrypted watermark image E[AW]. Then after recovery process and decryption is done to achieve image A and watermark image W. The proposed algorithm of watermarking in encrypted domain is shown in fig. 2.

4.1 Encryption Procedure

With the help of watermarking procedure transferring of digital media is secured. Watermarking procedure is carried out in an encryption domain. Figure 3 describes the encryption method for images. Following steps of embedding are described below

a.) Firstly, an original image is decomposed by using DWT to make the DWT coefficients like cA, cH, cV, cD sub bands.
b.) DCT is applied on each wavelet coefficients to achieve the DCT coefficients like cA' *(m, n),* cH' *(m, n),* cV' *(m, n),* cD' *(m, n).*
c.) Then scrambled image matrix and all DCT coefficients are undergoes for encryption process.
Watermark embedding is done by following equation:

$$P = Q + \alpha \times R \tag{12}$$

Figure 2. Block diagram of watermarking system
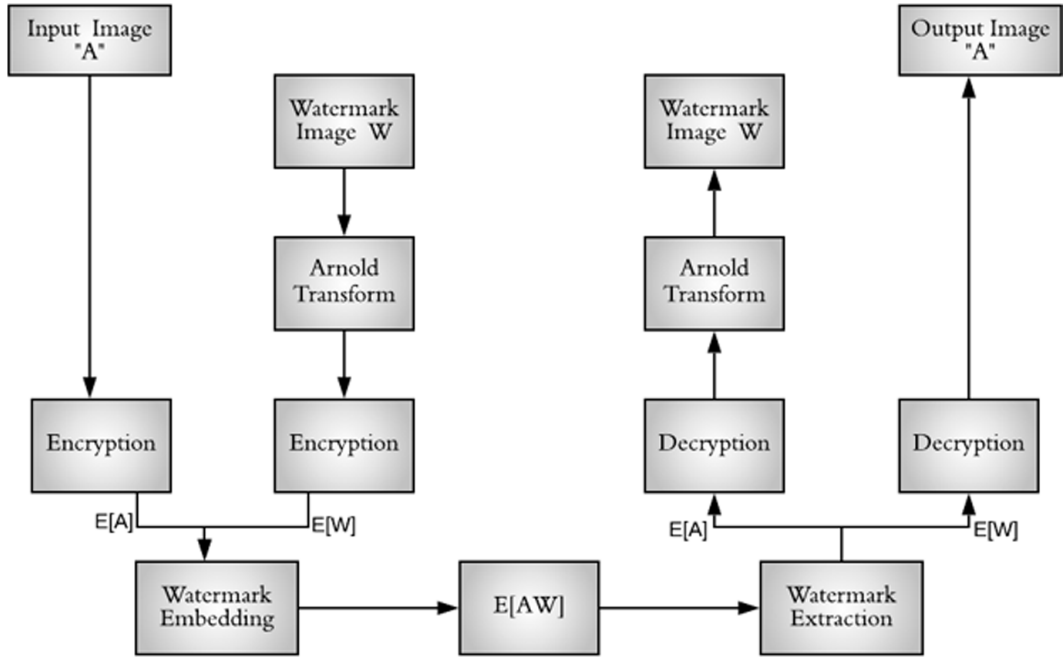
Where, α is gain factor. P is encrypted watermarked image, Q denotes encrypted original image and R represents watermark image, scrambled by Arnold scrambling.

e.) After that inverse DCT is applied then inverse DWT is implemented to get the encrypted image.
f.) Key is generating by using the XOR operation in between to encrypted image with scrambled image.
g.) Finally, the original media (image) is embedded with the watermark image.

4.2 Extraction Procedure

The extraction steps of watermarking system are just contrary of an embedding procedure.

a.) Now, decryption process is applied on encrypted image to get decrypted watermark image
b.) DWT transformation is applied on decrypted watermark image to get DWT coefficients cA1, cH1, cV1, cD1 sub-bands.
c.) DCT is applied on DWT coefficients to get DCT coefficients cA11 *(m, n),* cH11 *(m, n),* cV11 *(m, n),* cD11 *(m, n).*

Extract the watermark from embedded image by following equation:

$$x = \frac{y - z}{\alpha} \tag{13}$$

Where, α is a gain factor, *y* is matrix of encrypted watermarked image, *z* represents the encrypted original image and *x* is extracted watermark image.

e.)   Further process is pursued by inverse of DCT then IDWT to get extracted watermark image.

5. ANALYSIS SECTION

For our experiment we have used the size of cover and watermark images are 512 * 512 and 32*32 respectively. Some performance matrices like PSNR, NCC, NPCR and UACI are taken into consideration for our analysis. Detail explanation with equation is stated in next sub-section.

5.1 Performance Parameters

Some performance matrices like PSNR, NCC, NPCR and UACI are taken into consideration for our analysis. Detail explanation with equation is stated in next sub-section.

5.1.1 PSNR and NCC

Accomplishment of watermark embedding and extraction is done using peak signal to noise ratio (PSNR) and normalized cross-correlation (NCC). It illustrates the similarity between the embedded and recovered watermark images.

$$NCC = \frac{\sum_i \sum_j o(i,j) o'(i,j)}{\sum_i \sum_j o^2(i,j)} \tag{14}$$

The value of NCC is high then there is similarity between original and extracted watermarks. The PSNR is used to analyse the substantial distortion between original and watermarked images.

Figure 3. Encryption process
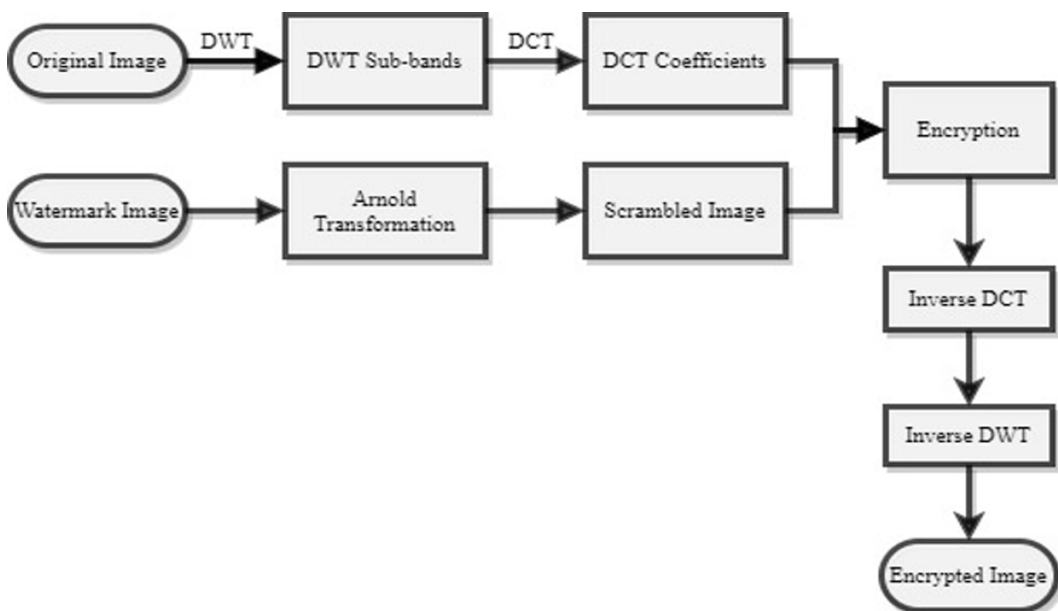
$$PSNR = 10\log_{10} \frac{max\left(I\left(i,j\right)\right)^2}{MSE} \tag{15}$$

Where i, j defines the pixel values of original images.

The MSE is calculated as difference between the pixel values of both original and watermarked images.

$$MSE = \frac{1}{MN}\sum_{i}\sum_{j}\left(C\left(i,j\right) - C'\left(i,j\right)\right)^2 \tag{16}$$

Where C and C' represents the original and watermarked images. M and N defines the row and column of the image matrix.

5.1.2 NPCR and UACI

NPCR actually finds the rate of change of pixels location among plain and encrypted image, whereas UACI is used to calculate the average difference between the input and encrypted image pixels in Khan et al. (2019). The NPCR and UACI can be described as follows:

$$B\left(i,j\right) = \begin{cases} 0, if\ E_1\left(i,j\right) = E_2\left(i,j\right) \\ 1, if\ E_1\left(i,j\right) \neq E_2\left(i,j\right) \end{cases}$$

$$NPCR = \sum_{i,j}\frac{B\left(i,j\right)}{T}X100\% \tag{17}$$

Where, E_1 and E_2 are the images before and after encryption. E_1 (i, j) and E_2 (i, j) are first pixel value at i, j coordinate. T represents the total number of pixels. And B denotes the bipolar array it has value 0 when pixels are same and value 1 when pixels are different.

$$UACI = \sum_{i,j}\frac{\left|E_1\left(i,j\right) - E_2\left(i,j\right)\right|}{P \cdot T} \times 100\% \tag{18}$$

Here, E_1 (i, j) and E_2 (i, j) represents the same as NPCR. P denotes the largest supported pixel value compatible to ciphertext image format.

Table 1 shows the Psnr and NC performance of our proposed algorithm. The best PSNR and ncc value is 56.98 and 0.9974 for the image Lena. However, the lower Psnr is 55.78 for the image football. And lower ncc value 0.9735 for the image Goldhill.

Figure 4 represents the experimental outcome of original and watermark image. Original image is undergone into encryption process and get encrypted image whereas watermark image is converted into scrambled watermark image through Arnold transformation. Further embedding operation is done to get the encrypted image.

Table 2 shows the outcome of NC value at different attacks. Here the noise density for Salt & Pepper and Gaussian Noise is 0.01. JPEG compression attack is tested under quality factor 90.

Table 1. Performance evaluation for different images

S.No.	Images	PSNR (DB)	NCC	NPCR	UACI
1	Lena	56.98	0.9974	0.9959	0.3444
2	Barbara	56.95	0.9968	0.9954	0.3737
3	Mandrill	56.55	0.9965	0.9959	0.4464
4	Peppers	56.12	0.9824	0.9961	0.4572
5	Football	55.78	0.9799	0.9958	0.4501
6	Goldhill	56.52	0.9735	0.9952	0.3735

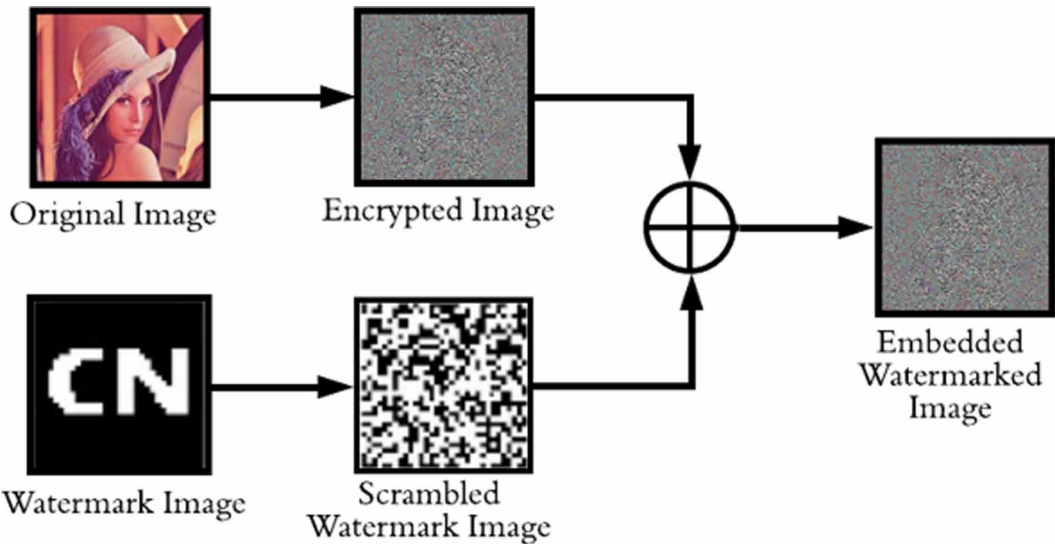Figure 4. Watermarking results for image Lena

Table 2. NC values tested at different attacks for different images

Image/ Attacks	Salt & Pepper Noise	Gaussian Noise	Filtering (3x3)	JPEG (90)	Rotation -300	Cropping
Lena	0.9785	0.9726	0.9684	0.9816	0.9678	0.9671
Barbara	0.9788	0.9732	0.9729	0.9821	0.9725	0.9745
Mandrill	0.9732	0.9719	0.9779	0.9799	0.9755	0.9722
Peppers	0.9685	0.9765	0.9712	0.9795	0.9682	0.9688
Football	0.9699	0.9722	0.9742	0.9818	0.9695	0.9674
Goldhill	0.9739	0.9715	0.9685	0.9789	0.9679	0.9669

Table 3 shows the assessment of psnr value of our approach with existing methods. And found that presented method found superior results than previous methods as well as more robust in nature. Figure 5 signifies the graphical representation of table 3.

Table 3. Comparison of PSNR value with other approach

Images	Proposed Method	Method of Su et al. (2018)	Method of Das et al. (2014)
Lena	56.98	49.98	41.78
Peppers	56.12	50.08	41.01

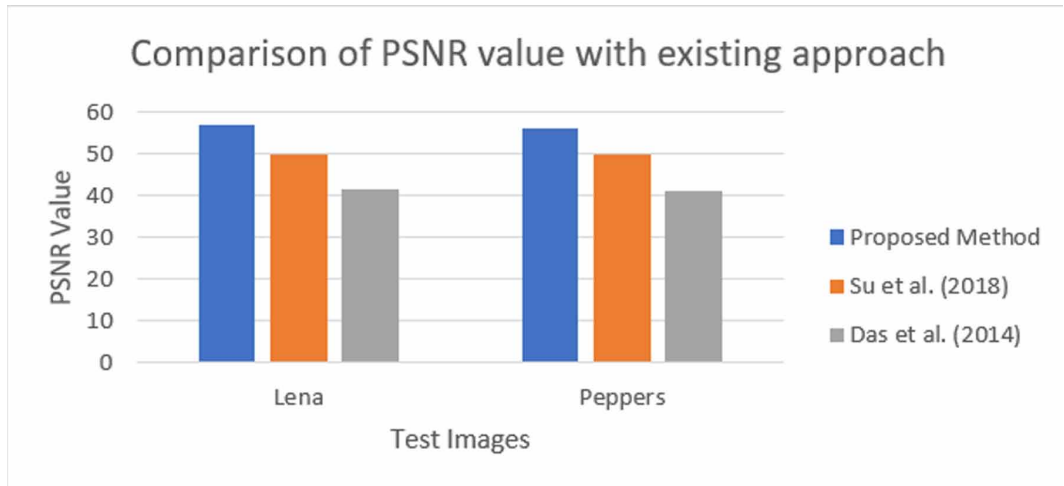**Figure 5. Graphical Representation of Proposed Approach with Existing Methods**

Table 4 shows the comparison of NC value under different attacks with existing methods. Presented watermarking method with encryption achieves good results in comparison to existing one.

6. CONCLUSION

An amended robust and secure watermarking approach in transform domain is offered. In this experiment, an improved algorithm for robust, imperceptible and secure image watermarking based on public key encryption (Pascal Paillier cryptosystem which is homomorphic and probabilistic) with Arnold transformation is used. The original media (image) and scrambled watermark image is encrypted before embedding process. Through decryption, watermark image is extracted from

Table 4. The comparison of NC values for different attacks with existing approach

S. No.	Images	Attacks/ Noise Density	Proposed Method	Method of Su et al. (2018)	Method of Das et al. (2014)
1	Lena	Salt & Pepper (0.01)	0.9785	0.9009	0.6731
2	Peppers		0.9685	0.9378	0.7866
3	Lena	Filtering (3x3)	0.9684	0.9977	0.9118
4	Peppers		0.9712	1	0.9233
5	Lena	Rotation (30⁰)	0.9678	0.7612	0.7612
6	Peppers		0.9682	0.7851	0.7851

encrypted watermarked image at extraction phase. Experimental discussion indicates that our method found robust and secure for different attacks also. It is observed that presented technique is superior than some existing approaches. We would like to further expansion of this work in future for video transmission system, medical image content and multiple watermarking.

REFERENCES

Abdallah, H. A., Ghazy, R. A., Kasban, H., Faragallah, O. S., Shaalan, A. A., Hadhoud, M. M., Dessouky, M. I., El-Fishawy, N. A., Alshebeili, S. A., & Abd El-samie, F. E. (2014). Homomorphic image watermarking with a singular value decomposition algorithm. *Information Processing & Management*, *50*(6), 909–923. doi:10.1016/j.ipm.2014.07.001

Agradriya, B. A., Safitri, I., Novamizanti, L., & Yaqin, M. A. (2019, March). Copyright Protection High Robustness Arnold Transform Wavelet Method. In *2018 International Conference on Industrial Enterprise and System Engineering (ICoIESE 2018)*. Atlantis Press. doi:10.2991/icoiese-18.2019.16

Ali, M., & Ahn, C. W. (2018). An optimal image watermarking approach through cuckoo search algorithm in wavelet domain. *International Journal of System Assurance Engineering and Management*, *9*(3), 602–611. doi:10.1007/s13198-014-0288-4

Aslantas, V. (2008). A singular-value decomposition-based image watermarking using genetic algorithm. *AEÜ. International Journal of Electronics and Communications*, *62*(5), 386–394. doi:10.1016/j.aeue.2007.02.010

Atawneh, S., Almomani, A., Al Bazar, H., Sumari, P., & Gupta, B. (2017). Secure and imperceptible digital image steganographic algorithm based on diamond encoding in DWT domain. *Multimedia Tools and Applications*, *76*(18), 18451–18472. doi:10.1007/s11042-016-3930-0

Boussif, M., Aloui, N., & Cherif, A. (2018). Secured cloud computing for medical data based on watermarking and encryption. *IET Networks*, *7*(5), 294–298. doi:10.1049/iet-net.2017.0180

Chang, C. C., Chen, K. N., Lee, C. F., & Liu, L. J. (2011). A secure fragile watermarking scheme based on chaos-and-hamming code. *Journal of Systems and Software*, *84*(9), 1462–1470. doi:10.1016/j.jss.2011.02.029

Das, C., Panigrahi, S., Sharma, V. K., & Mahapatra, K. K. (2014). A novel blind robust image watermarking in DCT domain using inter-block coefficient correlation. *AEÜ. International Journal of Electronics and Communications*, *68*(3), 244–253. doi:10.1016/j.aeue.2013.08.018

Eyadat, M., & Vasikarla, S. (2005). Performance evaluation of an incorporated DCT block-based watermarking algorithm with human visual system model. *Pattern Recognition Letters*, *26*(10), 1405–1411. doi:10.1016/j.patrec.2004.11.027

Gupta, R., Mishra, A., & Jain, S. (2018). A semi-blind HVS based image watermarking scheme using elliptic curve cryptography. *Multimedia Tools and Applications*, *77*(15), 19235–19260. doi:10.1007/s11042-017-5351-0

Horng, S. J., Rosiyadi, D., Fan, P., Wang, X., & Khan, M. K. (2014). An adaptive watermarking scheme for e-government document images. *Multimedia Tools and Applications*, *72*(3), 3085–3103. doi:10.1007/s11042-013-1579-5

Hsu, C. S., & Tu, S. F. (2010). Probability-based tampering detection scheme for digital images. *Optics Communications*, *283*(9), 1737–1743. doi:10.1016/j.optcom.2009.12.073

. Jost, C., Lam, H., Maximov, A., & Smeets, B. J. (2015). Encryption Performance Improvements of the Paillier Cryptosystem. *IACR Cryptol. ePrint Arch., 2015*, 864.

Kaur, A., Singh, P., & Nayyar, A. (2020). Robust Multimedia Watermarking: Characteristics, Applications, and Attacks. In Handbook of Research on Multimedia Cyber Security (pp. 73-89). IGI Global.

Khan, M., & Masood, F. (2019). A novel chaotic image encryption technique based on multiple discrete dynamical maps. *Multimedia Tools and Applications*, *78*(18), 26203–26222. doi:10.1007/s11042-019-07818-4

Li, J., Lin, Q., Yu, C., Ren, X., & Li, P. (2018). A QDCT-and SVD-based color image watermarking scheme using an optimized encrypted binary computer-generated hologram. *Soft Computing*, *22*(1), 47–65. doi:10.1007/s00500-016-2320-x

Lin, S. D., Shie, S. C., & Guo, J. Y. (2010). Improving the robustness of DCT-based image watermarking against JPEG compression. *Computer Standards & Interfaces*, *32*(1-2), 54–60. doi:10.1016/j.csi.2009.06.004

Liu, R., & Tan, T. (2002). An SVD-based watermarking scheme for protecting rightful ownership. *IEEE Transactions on Multimedia*, *4*(1), 121–128. doi:10.1109/6046.985560

Liu, Y., Tang, S., Liu, R., Zhang, L., & Ma, Z. (2018). Secure and robust digital image watermarking scheme using logistic and RSA encryption. *Expert Systems with Applications*, *97*, 95–105. doi:10.1016/j.eswa.2017.12.003

Liyun, S., Hong, M. A., & Shifu, T. (2006). Adaptive image digital watermarking with DCT and FCM. *Wuhan University Journal of Natural Sciences*, *11*(6), 1657–1660. doi:10.1007/BF02831844

Loukhaoukha, K., Nabti, M., & Zebbiche, K. (2014). A robust SVD-based image watermarking using a multi-objective particle swarm optimization. *Opto-Electronics Review*, *22*(1), 45–54. doi:10.2478/s11772-014-0177-z

Maity, S. P., & Kundu, M. K. (2011). Perceptually adaptive spread transform image watermarking scheme using Hadamard transform. *Information Sciences*, *181*(3), 450–465. doi:10.1016/j.ins.2010.09.029

Nikolaidis, N., & Pitas, I. (1998). Robust image watermarking in the spatial domain. *Signal Processing*, *66*(3), 385–403. doi:10.1016/S0165-1684(98)00017-6

Patel, S. B., Mehta, T. B., & Pradhan, S. N. (2011). A unified technique for robust digital watermarking of colour images using data mining and DCT. *International Journal of Internet Technology and Secured Transactions*, *3*(1), 81–96. doi:10.1504/IJITST.2011.039680

Priya, S., Varatharajan, R., Manogaran, G., Sundarasekar, R., & Kumar, P. M. (2018). Paillier homomorphic cryptosystem with poker shuffling transformation based water marking method for the secured transmission of digital medical images. *Personal and Ubiquitous Computing*, *22*(5-6), 1141–1151. doi:10.1007/s00779-018-1131-8

Rawat, S., & Raman, B. (2012). A publicly verifiable lossless watermarking scheme for copyright protection and ownership assertion. *AEÜ. International Journal of Electronics and Communications*, *66*(11), 955–962. doi:10.1016/j.aeue.2012.04.004

Santhi, V., & Arulmozhivarman, P. (2013). Hadamard transform based adaptive visible/invisible watermarking scheme for digital images. *Journal of Information Security and Applications*, *18*(4), 167–179. doi:10.1016/j.istr.2013.01.001

Seong, T. Y., Kwon, K. C., Lee, S. H., Moon, K. S., & Kwon, K. R. (2014). DCT and Homomorphic Encryption based Watermarking Scheme in Buyer-seller Watermarking Protocol. *Journal of Korea Multimedia Society*, *17*(12), 1402–1411. doi:10.9717/kmms.2014.17.12.1402

Singh, A. K., Dave, M., & Mohan, A. (2014). Hybrid technique for robust and imperceptible image watermarking in DWT–DCT–SVD domain. *National Academy Science Letters*, *37*(4), 351–358. doi:10.1007/s40009-014-0241-8

Singh, D., & Singh, S. K. (2017). DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection. *Multimedia Tools and Applications*, *76*(11), 13001–13024. doi:10.1007/s11042-016-3706-6

Su, Q., & Chen, B. (2018). Robust color image watermarking technique in the spatial domain. *Soft Computing*, *22*(1), 91–106. doi:10.1007/s00500-017-2489-7

Su, Q., Niu, Y., Zhao, Y., Pang, S., & Liu, X. (2013). A dual color images watermarking scheme based on the optimized compensation of singular value decomposition. *AEÜ. International Journal of Electronics and Communications*, *67*(8), 652–664. doi:10.1016/j.aeue.2013.01.009

Trivedy, S., & Pal, A. K. (2017). A logistic map-based fragile watermarking scheme of digital images with tamper detection. *Iranian Journal of Science and Technology. Transaction of Electrical Engineering*, *41*(2), 103–113. doi:10.1007/s40998-017-0021-9

Vahedi, E., Zoroofi, R. A., & Shiva, M. (2012). Toward a new wavelet-based watermarking approach for color images using bio-inspired optimization principles. *Digital Signal Processing*, *22*(1), 153–162. doi:10.1016/j.dsp.2011.08.006

Xianghong, T., Shuqin, X., & Qiliang, L. (2003, December). Watermarking for the digital images based on model of human perception. In *International Conference on Neural Networks and Signal Processing, 2003. Proceedings of the 2003* (Vol. 2, pp. 1509-1512). IEEE. doi:10.1109/ICNNSP.2003.1281162

Zhang, Z., Wang, C., & Zhou, X. (2016, November). Image watermarking scheme based on Arnold transform and DWT-DCT-SVD. In *2016 IEEE 13th International Conference on Signal Processing (ICSP)* (pp. 805-810). IEEE. doi:10.1109/ICSP.2016.7877942

Namita Agarwal is working as a full time PhD Scholar at Jaypee University of Information Technology, Waknaghat, India. He has published many papers and his one of the paper is published in Multimedia Tools and Applications (SCI, Springer) Journal based on his PhD research work.

Pradeep Kumar Singh is currently working as Assistant Professor (Senior Grade) in Department of Computer Science & Engineering at Jaypee University of Information Technology (JUIT), Waknaghat, India. He has 10 years of vast experience in academics at reputed colleges and universities of India. He has completed his Ph.D. in Computer Science & Engineering from Gautam Buddha University (State Government University), Greater Noida, UP, India. He is having life membership of Computer Society of India (CSI) and promoted to Senior Member Grade. He is a senior member of ACM, IACSIT-Singapore and IAENG-Hong Kong. He is associated with many IEEE International Conferences as TPC member, reviewer and session chair. He is Associate Editor of International Journal of Information Security and Cybercrime (IJISC) a peer-reviewed journal. He has published nearly 50 research papers in various Scopus, SCI Journals, and Conferences of repute. He has organized various theme-based special sessions during the International conferences also. He has three sponsored research project in his account. His research interest includes wireless sensor networks, IoT, data mining and optimization techniques.