An Efficient and Secure Certificateless Public Key Watermarking Scheme Based on SVD-DWT

Osman Wahballa[1,2], Ahmed Abdalla[1,2], Khalid Hamdnaalla[2], Mohammed Ramadan[1,2], Chunxiang Xu[1]
[1]School of Computer Science and Engineering, University of Electronic Science and Technology of China, 610054 Chengdu, China
[2]School of Electrical and Computer Engineering, Karary University, Khartoum, Sudan
e-mail: {wahballa_777, ahmed.baoney6}@hotmail.com; {jacobyousif135, nopatia}@gmail.com; chxxug@uestc.edu.cn

***Abstract*—Security and robustness are the main significant properties in watermarking system. In this paper, we propose an effective and secure certificateless public key watermarking scheme based on Singular Value Decomposition (SVD) and Discrete Wavelet Transform (DWT). The proposed method guarantees the non prior knowledge two parties to communicate covertly over an insecure and public channel. Moreover, we examine the robustness of the proposed scheme by analyzing different, original and watermarking images. The results demonstrate that our scheme fulfills all the security requirements of watermarking system and it is a powerful against various types of advanced attacks.**

Keywords-certificateless public key watermarking; discrete wavelet transform; singular value decompositions

I. INTRODUCTION

In recent times, the Internet has become the backbone for the transmission and reception of data around the world. Due to the extraordinary rate with which the internet expands, it is no longer just an avenue through which military or the research groups communicate, but a channel of communication that permeates all facets of life from homes to offices and other business areas [1], [2].

The Internet is now a major conduit through which large amounts of intellectual property are conveyed globally, and as the multimedia industry grows, it raises concern about the problems of copyright protection and content authentication. Keeping multimedia product rights away from illegal distribution and reproduction becomes a very big concern to its original authors and inventors. On the other hand, the receivers of the multimedia products want assurance of the integrities and authenticities of the products [3]. For all of that, communication security becomes a major concern. In order to resolve this problem, various kinds of watermarking are proposed, but only a few introduce multipurpose watermarking. Public-key watermarking has the function both of the robust watermark and the fragile one, which can resist malicious attacks and locate the area that is altered. It is much more effective in some special instances. The block diagram of the different embodiment disciplines of information hiding is shown in Fig. 1.

In this paper, an efficient certificateless public key watermarking scheme is proposed, where the authentication watermark and the robust watermark are both embedded in the SVD-DWT [4]. In addition, in order to strengthen the security, the watermarking algorithm still utilizes the Certificateless Public Key cryptosystem and the error correction coding. The advantage of public-key cryptosystem is that no one can destroy the watermark or get the original un-watermarked image without the owner's private key.

Through a series of experiments, supportive evidence was provided to demonstrate the proposed method being effective in image authentication and resisting image processing attacks.

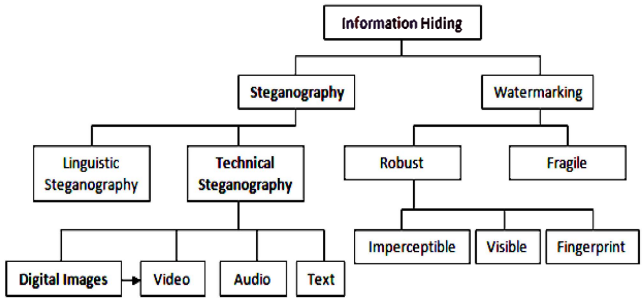

Figure 1. The different embodiment disciplines of information hiding.

II. RELATED WORK

The key technology by Wong algorithm is the basis of block wise image authentication algorithms, which divides the image into several non overlapping blocks. Therefore, for each block, the block signature is calculated via public key hash function and inserted into the Least Significant Bits (LSBs) of the same block [5]. Unfortunately, the block wise algorithms are weak against vector quantization attacks [6] that can produce a watermarked image or add/remove objects to/from it. Besides, still effectively pass the verification process as authentic.

The algorithm restrictions and achievable attacks are addressed in [7], [8]. The most serious threat is that, the attacker can replace without verification triggering. In doing so, it is vulnerable to falsification attacks.

In [9], an algorithm has been proposed to utilize quantized coefficients of the Discrete Cosine Transform (DCT) of the image blocks as a watermark and adjust the coefficient differences to resemble the quantized coefficients. However, the attacker can simply overcome the verification process by employing the similar algorithm to a fake image.

In [8], a perfect algorithm is presented, which makes use of a halftone version of the host image as an alternative of using the JPEG compression version. The halftone image is pixel-wise permuted by means of a random generator and embedded into the LSBs of the original image.

Obviously, the security of this algorithm lies in the key of the random generator, which may be detected using cryptographic analysis if the attacker has many authenticated images [10], [11]. In [12], the fractal codes of the region of interest (ROI), which are chosen as the important object in the image, are used as an approximated version of the ROI. The codes and a watermark are inserted into the LSBs of the host image.

Fridrich et al. [13] proposed a reversible authentication technique for images based on lossless bit-plane compression. They used the lowest bit-plane that provides enough space for the image hash after lossless compression. The disadvantage of this method is that for some noisy images we may have to use higher bit-planes and the distortion due to authentication can become visible.

Wong proposed a secret key watermarking scheme [14] and a public key watermarking scheme [15] for image authentication. These schemes allow a user with an appropriate key to verify the integrity and the ownership of an image Furthermore; this authentication watermark can detect and localize any change to the image, including changes in pixel values or image size. The security of these two schemes resides in the secrecy of the user key and not in the obscurity of the algorithm. In fact, the watermark insertion and extraction steps can be made public without compromising the security of the watermark.

A hybrid private-key image authentication technique has recently been proposed in [16]. This method includes a robust self-embedding scheme for self-correction and a fragile scheme for sensitive authentication. The main problem of this algorithm is the low quality of the authenticated image and/or reconstructed image.

- Discrete Wavelet Transform (DWT): The digital wavelet transform are scalable in nature. DWT more frequently used in digital image watermarking because of its excellent spatial localization and multi resolution techniques. The excellent spatial localization property is very convenient to recognize the area in the cover image in which the watermark is embedded efficiently [17].

The DWT is applied on the host image to decompose the image into four non overlapping multi resolution coefficient sets. The coefficients are:

$$W_{LL}^{J} = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} g(x)g(y)W_{LL}^{J-1}(2u-x)(2v-y) \qquad (1)$$

$$W_{LH}^{J} = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} g(x)h(y)W_{LL}^{J-1}(2u-x)(2v-y) \qquad (2)$$

$$W_{HH}^{J} = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} h(x)h(y)W_{LL}^{J-1}(2u-x)(2v-y) \qquad (3)$$

where J is the level of the 2-D DWT, $h(n)$ and $g(n)$ are the impulse response.

- Singular value decomposition (SVD): Singular value decomposition is a linear algebra technique used to solve many mathematical problems [18]. Any image can be considered as a square matrix without loss of generality. So SVD technique can be applied to any kind of images.

The SVD belongs to orthogonal transform which decompose the given matrix into three matrices of same size [19]. To decompose the matrix using SVD technique it need not be a square matrix. Let us denote the image as matrix A. The SVD decomposition of matrix A is given using equation below

$$A = USV^{T} \qquad (4)$$

U and V are unitary matrices such that

$$U * U^{T} = 1$$

$$V * V^{T} = 1$$

where, I is an Identity matrix.

III. PROPOSED MODEL

In this section, we propose a public key certificateless watermarking method. The symbols of our proposed model are expressed in Table I. Meanwhile, the proposed model is described in diagram for more clearness as shown in Fig. 2.

As customary, Alice and Bob are in prison, and want to relay information between them using a public channel under the watch of a warden name by Wendy.

To avoid Wendy's control, Alice sends to Bob some harmless contents. Alice is said to be active when she embeds a hidden message $\mathbf{h_{img}}$ modifying the cover-image $\mathbf{C_{img}}$ into embed-image $\mathbf{w_{img}}$. Alice is not active when she sends truly harmless contents.

TABLE I. NOTATIONS OF PROPOSED SCHEME

Notation	Meaning
KGC	A key generation center
IDA	Alice's A's Identity
IDB	Bob's B's Identity
PA	Alice's public key
P_B	BOB'S public key
P_{PUB}	The KGC's master key
X_A	Alice's secret value
X_B	Bob's secret value
S_A	Alice's private key
SB	Bob's private key
DA	Alice's partial private key
DB	Bob's partial private key
SK	Shared secret key
H_{IMG}	A hidden-image (watermarking message)
C_{IMG}	A cover content
W_{IMG}	watermarking content
H_1, H_2	Two hash functions
£	Embedding algorithm
B	Extract algorithm

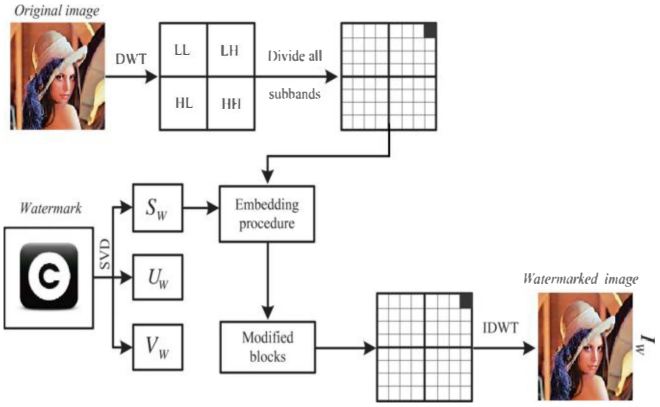

Figure 2. Process steps toward the watermarking image.

In order to establish a secure communication channel between Alice and Bob, we describe the eight algorithms needed to define our scheme based on Alriyami and Paterson [20] and He et al. [21] schemes, which include: Setup, Set Secret Value, Partial Private Key Extract, Set Private key, Set Public Key, Key-Agreement, embed and extract.

1) **Setup:** Initially, the **KGC** inputs the security parameters These include the topple $\{\mathbf{F_q}, \mathbf{E\backslash F_q}, \mathbf{G}, \mathbf{P}\}$as defined in Fig. 3

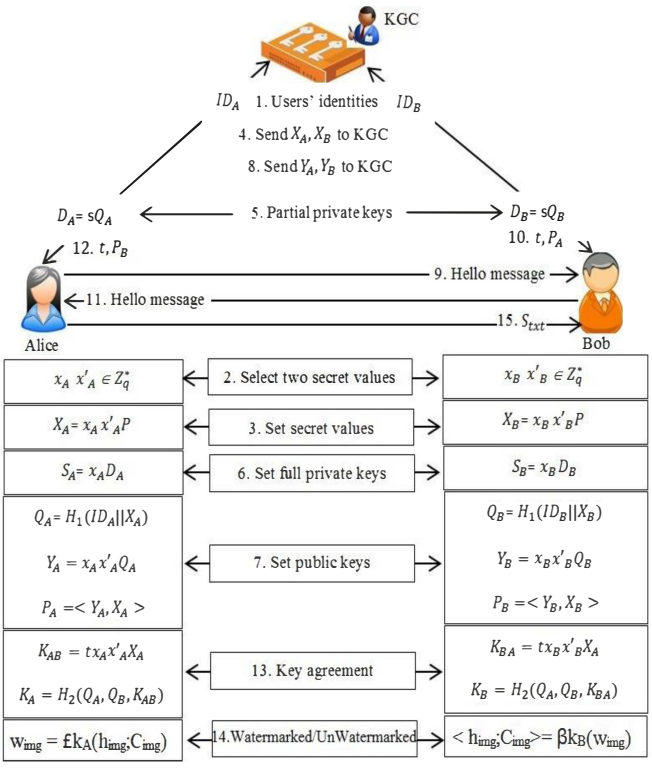

Figure 3. Proposed model diagrammatic description.

The KGC randomly chooses its master-key $s \in \mathbf{Z_n}^*$ and computes its public master-key $\mathbf{P_{pub}}=s\mathbf{P}$, and chooses two hash functions $\mathbf{H_1}:\{0,1\}^* \rightarrow \mathbf{Z_n}$ and $\mathbf{H_2}:\{0,1\}^* \rightarrow \mathbf{Z_n}$.

Finally, the **KGC** publishes the system parameters:

$$\text{Params}=(\mathbf{F_q}, \mathbf{E\backslash F_q}, \mathbf{G}, \mathbf{P}, \mathbf{P_{pub}}, \mathbf{H_1}, \mathbf{H_2},)$$

2) **Set Secret Value:** Alice A with identity $\mathbf{ID_A}$ selects $x_A \in \mathbf{Z_n}^*$ and sets x_A as secret value.

3) **Partial Private Key Extract**: **KGC** computes the partial private key of Alice with identity $\mathbf{ID_A}$ as follows:

- **KGC** chooses $\tau_A \in \mathbf{Z_n}^*$ computes: $\mathbf{R_A} = \tau_A \mathbf{P}$ and $h_A = \mathbf{H_1}(\mathbf{ID_A};\mathbf{R_A})$;
- Then, **KGC** computes $s_A = \tau_A + h_A \ s \bmod n$;
- **KGC** sets the tuple $\mathbf{D_A} = (s_A, R_A)$ as partial private key
- **KGC** sends $\mathbf{D_A}$ secretly to Alice.

4) **Set Private key:** When Alice receives $\mathbf{D_A}$ from the **KGC**, Alice can validate the partial private key by checking whether the equation $s_A\mathbf{P} = R_A + h_A\mathbf{P_{pub}}$ holds. If it holds, then Alice sets the pair $\mathbf{S_A} = (x_A;\mathbf{D_A})$ as her full private key.

5) Set Public Key: Alice computes her public key as

$$\mathbf{P_A} = x_A\mathbf{P}$$

Bob with identity $\mathbf{ID_B}$ can repeat algorithms from 2 to 5 to generate his keys.

6) **Key-Agreement:** The common authenticated per session secret key can be computed at both sides as follow:

- Alice sends $\mathbf{M_1} = (\mathbf{ID_A}, \mathbf{R_A}, \mathbf{P_A})$ to Bob;
- Upon Bob receiving $\mathbf{M_1}$, he chooses at random the ephemeral key $b \in \mathbf{Z_n}^*$ and computes $\mathbf{T_B} = b(\mathbf{P_A} + \mathbf{R_A} + \mathbf{H_1}(\mathbf{ID_A},\mathbf{R_A})\mathbf{P_{pub}})$. Then, Bob sends $\mathbf{M_2} = (\mathbf{ID_B},\mathbf{R_B},\mathbf{P_B},\mathbf{T_B})$ to Alice;
- After receiving $\mathbf{M_2}$, Alice chooses at random the ephemeral key $a \in \mathbf{Z_n}^*$ and computes $TA = a(\mathbf{P_B} + \mathbf{R_B} + \mathbf{H_1}(\mathbf{ID_B},\mathbf{R_B})\mathbf{P_{pub}})$. Then, Alice sends $\mathbf{M_3} = (\mathbf{T_A})$ to Bob;
- Then, both sides can compute the shared secrets as follows:
  - Alice computes $\mathbf{K^1_{AB}} = (x_A+s_A)^{-1}\mathbf{T_B}+a\mathbf{P}$ and $\mathbf{K^2_{AB}} = a(x_A + s_A)^{-1}\mathbf{T_B}$;
  - Bob computes $\mathbf{K^1_{BA}} = (x_B + s_B)^{-1}\mathbf{T_A} + b\mathbf{P}$ and $\mathbf{K^2_{BA}} = b(x_B + s_B)^{-1}\mathbf{T_A}$.
- Eventually, Alice and Bob can compute the shared secret keys as:

$$sk = \mathbf{H_2}(\mathbf{ID_A}||\mathbf{ID_B}||\mathbf{T_A}||\mathbf{T_B}||\mathbf{K^1_{AB}}||\mathbf{K^2_{AB}})$$
$$= \mathbf{H_2}(\mathbf{ID_A}||\mathbf{ID_B}||\mathbf{T_A}||\mathbf{T_B}||\mathbf{K^1_{BA}}||\mathbf{K^2_{BA}})$$

7) **Watermarking**: If Alice want to send secret image $\mathbf{h_{img}}$ (watermarking message) to Bob into cover-content $\mathbf{C_{img}}$ she can execute the following algorithm shown diagrammatically in Fig 2:

- Alice embeds a secret message $\mathbf{h_{img}}$ into watermarking-content $\mathbf{w_{img}}$ by modifying the cover-content $\mathbf{C_{img}}$ as: $\mathbf{w_{img}} = £k_A(\mathbf{h_{img}};\mathbf{C_{img}})$, where is £ the embedding algorithm;
- Then, Alice sends the $\mathbf{w_{img}}$ to Bob.

8) **Un-watermarking**: Bob extract Alice's watermarked image with shared key as follows: $\mathbf{< h_{img};C_{img} >= \beta k_B(w_{img})}$.

- **Correctness**

It can be easily seen that K^1_{AB} K^1_{BA} and K^2_{AB} K^2_{BA}. Hence, the shared secrets are agreed.

K^1_{AB} $(x_A + s_A)^{-1}T_B + aP$
$bP + aP$
K^1_{BA} $(x_B + s_B)^{-1}T_A + bP$
$aP + bP$
K^2_{AB} $a(x_A + s_A)^{-1}T_B$
abP
K^2_{BA} $b(x_B + s_B)^{-1}T_A$
$= baP$

IV. EXPERIMENTAL RESULTS

A. Evaluation Parameters

Herein, we show that, the proposed method is powerful and robust against different types of attacks. Accordingly, the watermarked image is subjected to different types of attacks which include Scaling, Blurring, Sharpening and Salt-and-Pepper noise .

Subsequently, the Peak Signal to Noise Ratio (PSNR).Normalized Correlation (NC), and Similarity Index (SI) values of the extracted watermark with respect to the original watermark are considered.

- Peak Signal-to-Noise Ratio: PPSNR is computed to examine the concealing effect of the watermark. It is calculated as the ratio between the maximum power of the original image and the power of unwanted noise which is added to the image yielding wrong exactness of image representation [22]. The mathematical representation can express by.

$$PSNR = 10\log_{10}\frac{M^2}{\frac{1}{m\times n}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j)-K(i,j)]^2} \quad (5)$$

where, M is the power of the signal, $I(i,j)$ is the original watermark and $K(i,j)$ is the extracted watermark. Bigger the PSNR value better the watermark conceals.

- Normalized Correlation: The robustness of the proposed algorithm is investigated by using the Normalized Cross Correlation (NC). It is a metric to assess the amount of similarity (or dissimilarity) between two compared images [23]. More precisely, we compare the original watermark to the extracted watermark. The equation to compute NC is given in below.

$$NC = \frac{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2}W(i,j)W'(i,j)}{\sqrt{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2}[W(i,j)]^2}\sqrt{\sum_{i=1}^{M_1}\sum_{j=1}^{M_2}[W'(i,j)]^2}} \quad (6)$$

where, $W(i,j)$ is the original watermark and ,$W'(i,j)$ is the extracted watermark. The value of NC is between 0 and 1. As the value increases, the method will be more robust.

- Structural Similarity Index (SI): is a measure of similarity between two images. It is also an indication of the quality measure of an image. Therefore, that image is compared with another image which is regarded as perfect quality image [24]. The equation to find out similarity index values is shown below.

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (7)$$

where μ_x is the average of x, μ_y is the average of y, σ_x^2 is the variance of x, σ_y^2 is the variance of y; σ_{xy} is the covariance of x and y; c_1 $(k_1L)^2$, c_2 $(k_2L)^2$, which are the two variables to stabilize the division; L is the dynamic range of pixel values and k_1 0.01 and k_2 0.03.

B. Results

The influence of the different types of attacks mentioned earlier are addressed against the watermarked image. The analysis is carried out by Matlab simulations. More precisely, different attacks are applied to the watermarked image and then, the watermark is extracted and the extracted watermark is compared in different viewpoints with the original watermark using the aforementioned evaluation parameters. The results obtained without and with different types of attacks are tabulated in Table II to Table VII.

TABLE II. RESULTS OBTAINED WITHOUT ATTACK

Image	PSNR	SSIM	NC
peppers	27.9346	0.9622	0.998
baboon	28.1024	0.9940	0.998
Lena	25.9209	0.9380	0.997

TABLE III. RESULTS OBTAINED WITH GAUSSIAN NOISE ATTACK

Image	PSNR	SSIM	NC
peppers	23.0316	0.8192	0.932
baboon	22.8087	0.8426	0.930
Lena	23.2586	0.8239	0.968

TABLE IV. RESULTS OBTAINED WITH PEPPER-SALT NOISE ATTACK

Image	PSNR	SSIM	NC
peppers	14.6607	0.5732	0.663
baboon	14.9506	0.5049	0.666
Lena	14.4107	0.4619	0.774

TABLE V. RESULTS OBTAINED WITH GAUSSIAN LOCALVAR NOISE ATTACK

Image	PSNR	SSIM	NC
peppers	14.0299	0.5828	0.594
baboon	12.4606	0.3805	0.531
Lena	12.8129	0.4835	0.711

TABLE VI. RESULTS OBTAINED WITH POISSON NOISE ATTACK

Image	PSNR	SSIM	NC
peppers	51.2929	0.9997	1.000
baboon	50.4628	0.9998	1.000
lena	53.9080	0.9998	1.000

TABLE VII. RESULTS OBTAINED WITH SPECKLE NOISE ATTACK

Image	PSNR	SSIM	NC
peppers	51.2929	0.9997	1.000
baboon	50.4628	0.9998	1.000
lena	53.9080	0.9998	1.000

From the results through Table II to Table VII, we can clearly see that, the PSNR values are comparatively high when there is no attack in the watermarked image. Also, the NC and SI values are close to 1, which indicates that, the method is robust enough and conceals better. After applying attacks, the PSNR values are not much reduced in most types of attacks and the NC and SI are relatively small as compared to a situation where there is no attack present. Fortunately, the results show that the proposed method is more robust against the Poisson noise attack and Speckle noise attack. Furthermore, NC and SI values are also enhanced in both attacks.

V. CONCLUSION

From the above descriptions, it have been shown that using singular value decomposition and discrete wavelet transform can ensure a secure certificateless public key watermarking. The proposed method has been described theoretically and diagrammatically. Besides, it is examined by applying different attacks and the performance is assessed by various factors included PSNR, NC and SI. The results have confirmed the effectiveness of the introduced method with and without the attacks. Remarkably, the method is more robust against the Poisson noise attack and Speckle noise attack.

REFERENCES

[1] P. Wang, L. Yao, L. Li. Adaptive digital watermarking algorithm combining spatial and DWT domain. *Optics and Precision Engineering*, 2006, 14(6): 1057-1062

[2] A. L. Oliveira, "Techniques for the Creation of Digital Watermarks in Sequential Circuit Designs", IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, Vol. 20, No. 9, September 2001, pp. 1101-1117.

[3] R G. van Schyndel, A Z. Tirkel, and D. Svalbe. Key Independent Watermark detection. IEEE International Conference on Multimedia Computing and Systems, 1999, vol. I, pp. 580-585.

[4] S. K. Prajapati, A. Naik and A. Yadav, "Robust Digital Watermarking using DWT-DCT-SVD",International Journal of Engineering Research and Applications, Vol. 2, Issue 3, May-Jun. 2012.

[5] N. Naveen Kumar, Dr.S.Ramakrishna, An Impressive Method to Get Better Peak Signal Noise Ratio (PSNR), Mean Square Error (MSE) Values Using Stationary Wavelet Transform (SWT), Global Journal of Computer Science and Technology Graphics & Vision, Volume 12, Issue 12, Version 1.0, 2012.

[6] Darshana Mistry, Comparison of Digital Watermarking methods, International Journal on Computer Science and Engineering, Vol. 02, No. 09, 2010, 2905-2909

[7] Mei Jiansheng, Li Sukang, Tan Xiaomei, A Digital Watermarking Algorithm Based on DCT and DWT, Proceedings of the InternationalSymposium on Web Information Systems and Applications, 2009, pp. 104-107.

[8] Po-Yueh Chen, Hung-Ju Lin, A DWT Based Approach for Image Steganography, International Journal of Applied Science and Engineering, 2006. 4, 3: 275-290

[9] Francois Cayre, Caroline Fontaine, Teddy Furon, Watermarking Security: Theory and Practice, IEEE Transactions on Signal Processing, Vol. 53, No. 10, 2005

[10] Du-Ming Tsai, Fast Normalized Cross Correlation for Defect Detection, November 2003.

[11] J. Jiang and A. Armstrong, A Data Hiding Approach for Efficient Image Indexing, IEEE Transaction, November 2002.

[12] Joachim J. Eggers, Jonathan K. Su, Attacks on Digital Watermarks: Classification, Estimation-Based Attacks, and Benchmarks, IEEE, 2001.

[13] J. Fridrich, M. Goldjan, and R. Du, "Invertible authentication," Proc. SPIE, Security and Watermarking of Multimedia Contents, pp. 197-208, Jan. 2001.

[14] P. W. Wong, "A watermark for image integrity and ownership verification," in Proceedings of IS&T PIC Conference, (Portland, OR), May 1998.

[15] P. W. Wong, "A public key watermark for image verification and authentication," in Proceedings of ICIP, (Chicago, IL), October 1998.

[16] Y. F.Chang, W. L.Tai, A block-based watermarking scheme for image tamper detection and self-recovery, Opto-Electronics Review, volume 21, pp. 182-190, June 2013.

[17] N. Chandrakar and J. Baggaa ,"Performance Comparison of Digital Image Watermarking Techniques: A Survey", International Journal of computer Application Technology and Research, vol. 2, no. 2, (2013), pp. 126-130.

[18] Ruizhen Liu and Tieniu Tan, Senior Member, IEEE 2002 An SVD-Based Watermarking Scheme for Protecting Rightful Ownership. IEEE Transactions On Multimedia, Vol. 4, No. 1, March 2002.

[19] V. Santhi and Arunkumar Thangavelu 2009. DWT-SVD Combined Full Band Robust Watermarking Technique for Color Images in YUV Color Space. International Journal of Computer Theory and Engineering, Vol. 1, No. 4, October 2009.

[20] S. S. Al-Riyami, and K. G. Paterson, "Certificate-less public key cryptography,"in Proceedings of the Cryptography (Asiacrypt'03), LNCS, 2894, pp. 452-473, Springer-Verlag, 2003.

[21] D. He, J. Chen, J. Hu , "A pairing-free certificateless authenticated key agreement protocol," International Journal of Communication Systems, vol. 25, no. 2, pp. 221-230, 2012.

[22] N. Naveen Kumar, Dr.S.Ramakrishna, An Impressive Method to Get Better Peak Signal Noise Ratio (PSNR), Mean Square Error (MSE) Values Using Stationary Wavelet Transform (SWT), Global Journal of Computer Science and Technology Graphics & Vision, Volume 12, Issue 12, Version 1.0, 2012.

[23] Mei Jiansheng, Li Sukang, Tan Xiaomei, A Digital Watermarking Algorithm Based on DCT and DWT, Proceedings of the International Symposium on Web Information Systems and Applications, 2009, pp. 104-107.

[24] Aparna, J. R., and Sonal Ayyappan. “Image Watermarking Using Diffie Hellman Key Exchange Algorithm”. Procedia Computer Science, 46 (2015): 1684-1691.