Authentication of Images through Lossless Watermarking (LWM) Technique with the aid of Elliptic Curve Cryptography (ECC)

Arathi Chitla
Associate Professor
Department of Computer Science & Engineering,
Telangana University, Nizamabad,
Andhra Pradesh, India.

M. Chandra Mohan
Associate Professor
Department of Computer Science and Engineering
JNTUH, Hyderabad,
Andhra Pradesh, India.

ABSTRACT
A novel lossless watermarking image authentication technique is proposed in this paper. The proposed method allows exact recovery of the original information from the image without loss in their quality. For authenticating the information, a well known Elliptic Curve Cryptography (ECC) is utilized. The ECC method authenticates the information by generating signature and signed messages. After the authentication process, the data embedding process is performed, in which the computed information is inserted into the image data. The data embedding process is accomplished by the well known LSB (least significant bit) modification, which embeds the information bits to the image data. Subsequently, the recovery and the verification processes are carried out to find out whether the watermarked image is authenticated or not. The effectiveness of the proposed technique using ECC image authentication along with lossless Least Significant Bit (LSB) data embedding is evaluated. Also, the proposed LWM image authentication technique is compared with the conventional LWM technique. The comparison result shows that our proposed technique can retrieve the image with high PSNR value than the image retrieved by the conventional technique.

Keywords
Lossless Watermarking (LWM), Elliptic Curve Cryptography (ECC), Signature Generation Algorithm, Raster Scanning, Image Authentication

1. INTRODUCTION
Nowadays due to the rapid expansion of the Internet, the access to multimedia information has become much easier [8]. Thus, the progress of digital multimedia technology is very crucial for preserving the multimedia data in internet [13]. In archaic period, the source or originator of manuscript or image has been recognized by using diverse kinds of handwritten signatures, seals, or watermarks. While, in digital world, digital technology for updating images has made it tricky to discriminate the visual truth [15]. The two most common multimedia security techniques are Watermarking and Cryptography. But, cryptography is an inefficacious technique because it does not provide permanent security for the multimedia data after delivering to the customers [9]. Digital watermarking technique provides copyright protection for the digital data [1] [12]. A digital watermark is proposed to complement cryptographic processes. It is a perceptible or preferably imperceptible identification code, which is permanently implanted in the data and it remains within the data after any decryption process [3] [16]. Digital watermarking should offer the qualities such as imperceptibility, heftiness, and protection of cover image [2] [11]. Watermarks may be visible or invisible. A visible mark can be easily detectable by observation, whereas an invisible mark is designed to be translucent to the observer and identified by means of signal processing methods [6] [5]. Recently, a number of research on this area focuses on invisible watermarks, those which are undetectable under normal viewing conditions.

The different techniques that are employed for invisible image watermarks can be separated into two categories: (i) spatial-domain watermarks, and (ii) transform-domain watermarks [7]. In spatial domain watermarking, the watermark is implanted via the pixel values of images. Several techniques are proposed in spatial domain, utilizing the luminance components, manipulating the Least Significant Bits as ideal locations for embedding, manipulating the intensity components, image differencing, and so on [17]. While, in frequency domain watermarking, the watermark is implanted by means of the frequency coefficients of images [10] and the transformation may be done through Discrete Cosine Transform, Discrete Wavelet Transform, Ridgelet Transform etc., [17]. Normally, the watermarking attacks are unintentional or intentional functions that replace, alter, or remove the inserted watermarks. Almost all of these attacks are emerged from the normal image processing operations namely, Cropping, Bending, Sharpening, Shifting, Darkening, Lightening, Histogram Equalization, Median Filtering, Rotating, Scaling, Skewing, Lossless and Lossy Compression [4]. The potency of any watermarking approach can be decided by its performance against intentional and unintentional attacks. All watermarking approaches need to be evaluated to determine its performance. Three factors that should be considered while appraising an image watermarking algorithm are,

- Capacity - the quantity of data that can be put into the watermark and retrieved without errors.
- Robustness - the resistance of the watermark to modifications of the original data such as compression, filtering, or cropping.
- Visibility - how easily the watermark can be recognized by the user.

The available techniques utilize diverse transform domains to implant the watermark inspired by the methods of information coding and image compression [14]. A number of researches have been done for the successful watermarking image authentication. Some of the most recent works available in the literature are reviewed in the following section.

2. RELATED WORKS
Soliman *et al.* [18] have presented a secure patient medical images and authentication technique that improves the security,

privacy, and integrity of medical images send via the Internet. They have proposed a watermarking by invoking particle swarm optimization (PSO) method in adaptive quantization index modulation and singular value decomposition together with DWT and DCT. The proposed technique has enhanced the watermarked image quality. The experimental results have revealed that the watermark produced by proposed algorithm was imperceptible to human eyes, robust against most common attacks and reliable enough for finding conspirators.

Umaamaheshvari *et al.* [19] have proposed a frequency domain watermarking approach for testing the integrity and accuracy of medical images. The proposed watermarking approach has utilized hybrid transform, which is the combination DCT and DWT. Initially, the original image has been decomposed by hybrid transform. Then, the watermark embedding and extraction have been carried out in frequency domain using the proposed approach. The watermark extraction has been compared with the original image for computing the structural similarity index measure (SSIM). Moreover, the experimental results have shown the efficacy of the proposed watermarking approach.

An image tamper detection technique based on 3 LSB (last significant bit) watermarking scheme has been proposed by Dadkhah *et al.* [20], which has ability to authenticate the digital image and identify the tamper locations precisely. In the proposed algorithm, a 12-bit watermark key has been generated from each block of host image and it has been inserted into the last three significant bit of each block. The proposed technique has enhanced tamper detection method devised by Prasad's in sense of tamper detection rate by 40 percent. The experimental results have obviously proved the competence of the proposed technique.

Sujatha *et al.* [21] have proposed a watermarking technique, where the low frequency subband of wavelet domain and the rescaled version of original image have been exploited in the watermark generation process. A scrambled version of watermark has been acquired via Arnold Transform. The operation of implanting and extraction of watermark have been carried out in high frequency domain of DWT because small alterations in this domain were not visible by human eyes. The watermarking technique deals with the extraction of the watermark information in the absence of original image, thus it was referred as blind watermarking. Also, the image quality has been measured by calculating the Peak Signal to Noise Ratio (PSNR) and Similarity Ratio (SR).

Khalifa *et al.* [22] have proposed an algorithm, where a casting operation of a binary message has been applied onto the wavelet coefficients of colored images decomposed at multi-level resolution. In the extraction stage, the original "unwatermarked" image has been utilized to calculate the embedded bit-stream. Experimental results have demonstrated the low distortion effect caused by the embedding approach of the proposed method. Moreover, the resultant watermarked-images were highly resistance to attacks such as JPEG compression and normal image processing operations such as sharpening, blurring, and image filtering. More simulations have been performed to analyze the performance of the proposed algorithm in comparison to similar transform-domain approaches.

Watermarking is a mechanism of embedding information (i.e. the information may be text, symbols or any credential data) into the multimedia data such as image, audio or video. Besides the other, nowadays the image watermarking plays a vital role because rather than the audio and video, the images are accessible widely in the internet. The watermark can be distorted on the communication path or due to any other distortions. These distortions may not be visible to the human visual system if the original image and the modified image are identical. But it is an important issue in the surveillance applications, it has to be sustained the image fidelity. For achieving this, image authentication is carried out, in which the reconstruction of original image is mandatory before the validation in literature. This may increase the computational necessity in case of failed verification. For performing this authentication process prior to the validation, a Public Key Infrastructure (PKI) is utilized in [23]. In [23], the public key authentication is not so efficient. Also in this public key authentication, different algorithms were utilized and each possesses different issues such as large key size, mass storage and etc. Large sized key in cryptographic system provides high security but takes high computational time in encryption and decryption operation and occupies high storage space. To overcome such aforementioned issues in the existing methods, here we proposed a novel lossless watermarking image authentication technique.

Thus, our proposed technique comprises four stages namely, information authentication by ECC, data embedding on image, information & image recovery, and verification. In data embedding stage, the proposed authentication technique inserts the signed massages into the image. Then, this watermarked image information and the original image are recovered and verified whether the watermarked image is authenticated or non-authenticated. The structure of the paper is as follows: Section 3 details the proposed LWM image authentication technique with equations and proper explanations. Section 4 discusses the implementation results, and Section 5 concludes the paper.

3. NOVEL LOSSLESS WATER MARKING IMAGE AUTHENTICATION TECHNIQUE (LWM)

Here, a method for authenticating the image using lossless water marking is being proposed. The proposed method provides high capacity host signal (information) and non altered image by implementing the elliptic curve cryptography and LSB method. The proposed LWM image authentication technique consists of four processing stages namely, i) information authentication, ii) data embedding on image, iii) information and image recovery, and iv)Verification. These four stages are consecutively preformed and obtained the watermarked and recovered images. Let us consider two users, u_1 and u_2. The user u_1 sends a watermarked image with an embedded message to user u_2. To authenticate the message, the user u_1 signs the message using its private key p_1. Then, the user u_1 embeds the signed message (i.e., the combination of message and signature) onto the image and sends it to the user u_2. The embedding process on the image is performed by LSB. The user u_2 gets the watermarked image and recovers the message and image only by using the public key of user u_1. Since the user u_2 knows the $u_1's$ public key, it can verify whether the message is actually send by u_1 or not. The structure of proposed novel technique is illustrated in Fig. 1.

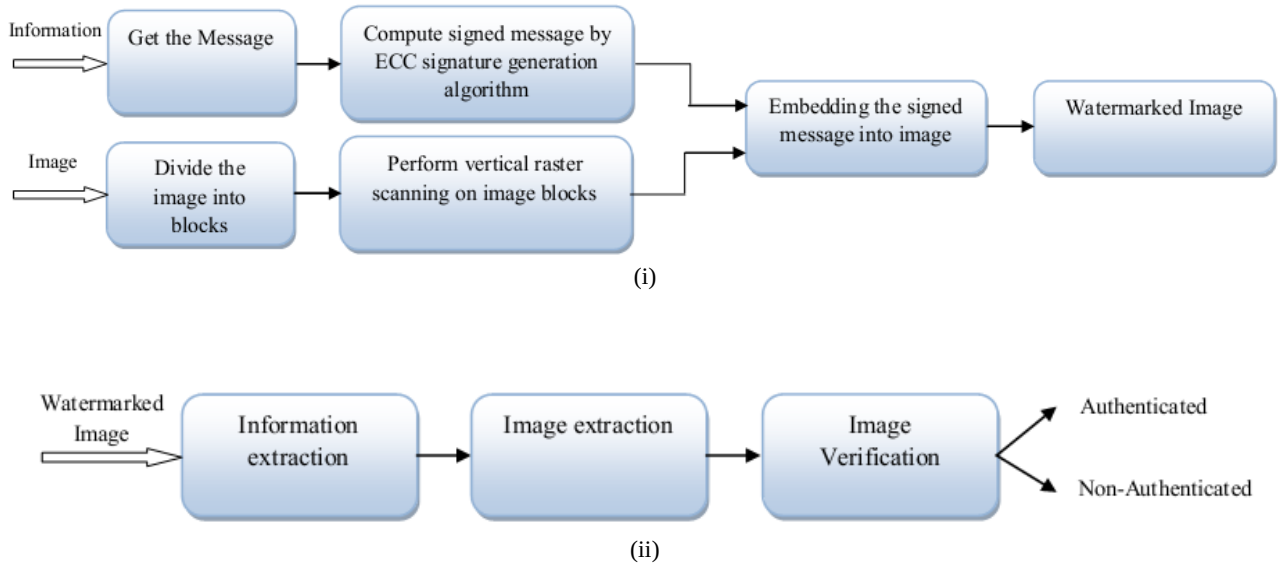

Fig 1: Structure of Proposed Image Authentication-Novel Lossless Water Marking Technique (i) Image Authentication and Embedding Process (ii) Recovery and Verification Process

Fig.1 (i) and (ii) shows our proposed lossless watermarking process for image authentication. Initially, we get the image and information as inputs. The given input image is divided into number of blocks and vertical raster scanning is performed on those blocks. The given input message is authenticated by the ECC signature generation algorithm and embedded this signed message into the image. Finally, we obtain the water marked image. The message and image extraction process is performed on the watermarked image and then, the extracted image is verified whether that image is authenticated or unauthenticated (i.e.) whether the received image is sent by the exact sender or not.

3.1 Information Authentication via Elliptic Curve Cryptography (ECC)

Here, we embed the massage (information) or host signal into an image by the elliptic curve cryptography. Elliptic Curve Cryptography (ECC) is also called as public key cryptography, where each user or the device participating in the communication usually have a couple of keys, a public key and a private key, and a set of operations related with the keys to do the cryptographic operations. Small key size is the main advantage of ECC. Here, we have performed the information authentication process by using ECC signature generation algorithm.

The operations of elliptic curve cryptography are defined over two finite fields: Prime field and Binary field. The suitable field is selected with finitely huge number of points for cryptographic operations. Here, we have used prime field operations by choosing a prime number N, and finitely large numbers of basic points are generated on the elliptic curve, such that the generated points are between 0 to N. Then, we randomly select one basic point $p_i(x_i, y_i)$ for cryptographic operations and this point satisfies the equation of the elliptic curve on a prime field, which is defined as

$$y^2 \bmod N = x^3 + ax + b \bmod N \quad (1)$$

In Equ. (1), are the parameters that defining the curve, and x *and* y are the coordinate values of the generated points p. We randomly select one basic point p_i that satisfies the aforementioned Equ. (1). To perform the cryptography, we need to select a private key p_k on the sender side, which is a randomly selected integer less than N and generate a public key $u_k = p_k * p_i$

Signature Generation: In signature generation, the sender A sends a message m to the receiver B by using its private key p_k, with a generated signature. The steps involved in signature generation are,

- Choose a random integer k from N (k<N, kis a prime number)
- Calculate $sg_l = k(m_l - p_k * x_j)$; here m_l represents the message bit and l is the number of characters in the message. (2)
- Compute $(x_j, y_j) = p_k * (x_i, y_i)$ (3)
- Generate signed message $s_m = (m_l, x_j, y_j), sg_l))$, If size s_m is not equal i.e., $s(m_l) \neq s(x_i) \neq s(y_i) \neq s(sg_l)$, then append zeros to the actual value in the affix.

3.2 Data Embedding on Image through Least Significant Bit (LSB)

In data embedding process, the signed message is embed into the image by using the LSB method. Initially, we divide the given input image I into M number of blocks I_M and select n number of pixels from every block by vertical raster scanning. Raster scanning is a method for generating or recording a video image by a line-by-line sweep, equivalent to a data mapping method between one and two dimensional spaces. While this geometric structure has been extensively employed on several data transmission and storage systems as well as most video displaying and capturing devices, its application to audio related research or art is rare. In this paper, we select n

pixels by performing vertical raster scanning. The n value computation is stated as,

$$n = \frac{4 * fs(s_m\ elements)}{M} \quad (4)$$

Increment the value of s_m elements s value by 1 until the condition given in Equ. (5) is satisfied.

$$(4 * s(s_m\ elements)) \bmod M = 0;\ increament\ s_m\ elements\ \ s \quad (5)$$

If the condition in Equ. (5) is satisfied in a certain s value, then we rearrange s_m elements size by the finally computed fs value. After the s_m elements size rearrangement and the n value computation process, we extract the n pixel values from each block in a vertical raster scanning approach. The extracted n pixel values corresponding binary values are computed and determined the least significant bit value (LSB) from each pixel binary value. The least significant bit values of each pixel from image I_M are replaced by the signed message s_m element values.

For example, consider a text message 'HELLO'. The ASCII value of each character is [72, 69, 76, 76, and 79] and the binary value is [01001000, 01000101, 01001100, and 01001111]. The signed message

$s_m = (01001000,01000101,01001100,01001111,$ Image pixel $00101100,01001100,00110010)$

values from block 1 are represented as (10000111, 10000110, 10000100, 10000001 (n=4)) and the least significant bit values are obtained and substituted as

10000111-> 10000110
10000110->10000111
10000100->10000100
10000001->10000000

Then, these values (10000110, 10000111, 10000100, and 10000000) are embedded into the image pixel values of block 1. Similarly, other blocks values are replaced by the signed messages. After the message embedding process, we obtain the water marked image I_w.

3.3 Information and Image Recovery

The information and image recovery process is performed over the watermarked image I_w. The receiver gets the water marked image I_w and performs the recovery process by extracting the image and the message embedded into the watermarked image. Image and information recovery process is described in the following steps.

- Divide the watermarked image I_w into M number of blocks, which is denoted as I_w^M.
- Perform vertical raster scanning process on the image I_w^M based on the n value.
- Get n pixels LSB value from M number of blocks image I_w^M.
- Divide this extracted LSB values into four parts with equal size. The first l parts are m_l, second 2 parts are (x_j, y_j), and the third l parts are sg_l.
- We compute the binary value m_l and then the ASCII value to retrieve the original image I.

3.4 Verification

Final stage in image authentication LWM technique is verification. The verification process is performed by the receiver B to check whether the received image I is send by the sender A or not. The receiver B performs the verification process by exploiting the public key u_k. Here, we perform the verification process by comparing two variables, which are calculated by using the public key and the basic point values. The comparison process is described below,

- Compute v_1,

$$v_1 = y_j(p_k * p_i) + s_m(x_j, y_j) \quad (6)$$

- Compute v_2,

$$v_2 = m_l * p_i \quad (7)$$

- If $v_1 = v_2$ then the image I is authenticated i.e. the image I is send by the sender A, otherwise the image is unauthenticated.

4. RESULTS AND DISCUSSION

The proposed LWM based image authentication technique is implemented in the working platform of MATLAB version 7.12. The given input information is authenticated by ECC and the authenticated message is embedding on the input image. The sender sends the watermarked image to the receiver. The receiver receives the watermarked image and check whether the received image is sent by the exact sender or not. The sample image utilized in the image authentication is shown in fig 2.

Fig 2: Sample Input Image

The input message is embedded into the sample image and we obtain the message embedded watermarked image, which is shown in Fig. 3.

Fig 3: Watermarked Image

Subsequently, we extract the image and the information from the watermarked image by using LSB method.

The extracted original image with PSNR value is illustrated in Fig. 4.

Fig 4: Receiver Extracted Image with PSNR value 75.22

The performance of our proposed method is analyzed by sending five numbers of watermarked images to the receiver.

The received image verification process is demonstrated in Table I.

Table 1. Performance Results of Proposed Image Authentication-LWM Technique

Message	Images	Retrieved Image PSNR value	Verification Results
HLO	1	75.22	Authenticated
	2	73.84	Authenticated
	3	73.84	Authenticated
	4	73.03	Authenticated
	5	71.47	Authenticated

4.1 Performance Analysis

The performance of our proposed technique is analyzed by comparing with the conventional lossless water marking authentication technique [24].The performance of both methods is evaluated by taking more number of images that are sent by the original sender and unknown persons. The performance of our proposed and conventional techniques for these authenticated and non-authenticated images in verification process is shown in Table II and III.

Table 2. Performance of Proposed Technique on Different Images from Original Sender and Unknown Persons

Images from original sender	PSNR value	Verification Results	Images from unknown person	PSNR value	Verification Results
	75.22	Authenticated		20.29	Authenticated
	73.84	Authenticated		20.46	Non-Authenticated
	73.84	Authenticated		20.27	Non-Authenticated
	73.03	Authenticated		24.17	Non-Authenticated
	71.47	Authenticated		20.50	Non-Authenticated

	72.21	Authenticated		20.99	Non-Authenticated
	70.98	Authenticated		23.12	Non-Authenticated
	70.59	Authenticated		22.53	Non-Authenticated
	70.28	Authenticated		22.61	Non-Authenticated
	70.32	Authenticated		20.28	Non-Authenticated

Table 3. Performance of Proposed Technique on Different Images from Original Sender and Unknown Persons

Images from original sender	**PSNR value**	**Verification Results**	**Images from unknown person**	**PSNR value**	**Verification Results**
	73.22	Authenticated		18.29	Authenticated
	70.84	Non-Authenticated		19.46	Non-Authenticated

	69.84	Non-Authenticated		20.27	Authenticated
	74.23	Authenticated		21.17	Non-authenticated
	67.47	Authenticated		20.50	Non-Authenticated
	71.21	Non-Authenticated		19.99	Authenticated
	68.98	Authenticated		21.12	Non-Authenticated
	69.59	Authenticated		20.53	Authenticated
	66.28	Authenticated		19.61	Non-authenticated
	69.32	Authenticated		20.28	Authenticated

As can be seen from table II and III, our proposed technique performance is high in terms of PSNR value and verification results than the conventional technique. Our proposed technique affords 40% higher performance than the conventional LWM image authentication technique in verification result from unknown person images. Also, the

verification results show that our proposed technique has accurately recognizes that the images authenticated or non-authenticated while the conventional technique has mistakenly produced the non-authenticated images as authenticated. The graphical representation of the proposed and conventional techniques comparison results is illustrated in Fig 5.

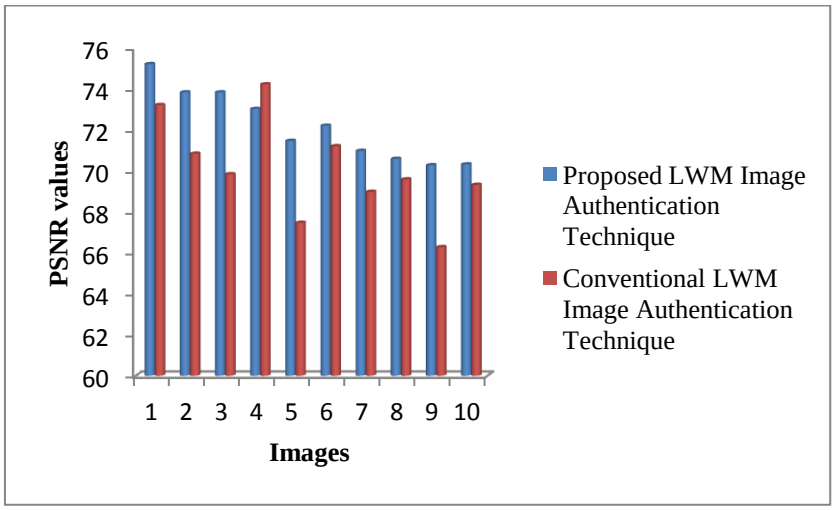

Fig 5: Comparison of Proposed and Conventional LWM Image Authentication Techniques in Terms of their PSNR values (images from original sender)

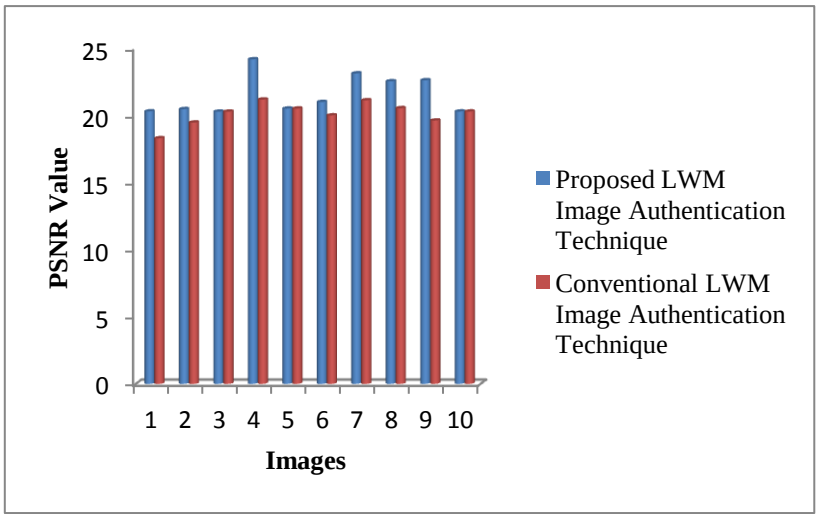

Fig 6: Comparison of Proposed and Conventional LWM Image Authentication Techniques in Terms of their PSNR Values (Images from Unknown Person)

Fig 5 and 6 shows the comparison result of the proposed and conventional LWM image authentication techniques in terms of their PSNR values with the images form original and unknown persons. The graphical representation shows that our proposed technique has yielded high PSNR value than the conventional technique. In fig. 5, the image 4 PSNR value of conventional technique is high than our proposed technique but this high level performance on single image does not affect our proposed technique efficiency. Hence, our proposed lossless watermarking image authentication technique provides high level performance in image authentication.

5. CONCLUSION

A novel lossless watermarking image authentication technique was proposed in this paper. The technique provides high embedding capacities, allows complete recovery of the original host signal, and the retrieved image have high PSNR value than the conventional technique. The PSNR value of the recovered image proves that the image was not altered and the lossless watermarking procedure was successfully implemented. The LWM image authentication with ECC and LSB has made our proposed technique robust over the conventional watermarking-authentication techniques. This novel lossless watermarking image authentication technique is enhanced in future works by exploiting the medical images.

6. REFERENCES

[1] Rosline Nesa Kumari, Vijaya Kumar, Sumalatha and Krishna, "Secure and Robust Digital Watermarking on Grey Level Images", International Journal of Advanced Science and Technology, Vol. 11, October, 2009

[2] Ashish Bansal , Sarita Singh Bhadauria, "Watermarking Using Neural Network and Hiding the Trained Network

within the Cover Image", Journal of Theoretical and Applied Information Technology, pp63-670, 2008

[3] A. Arulmurugan, N.Arul, P.Santhosh kumar, "Robust Image Watermarking in contourlet Domain Using Genetic Algorithm", Global Journal of Computer Science and Technology, Vol.11, No.9 , May 2011

[4] Mir Shahriar Emami, Ghazali Bin Sulong, "Set Removal Attack: A New Geometric Watermarking Attack", 2011 International Conference on Future Information Technology IPCSIT, vol.13, IACSIT Press, Singapore, 2011

[5] K.Ganesan and Tarun Kumar Guptha, "Multiple Binary Images Watermarking in Spatial and Frequency Domains", Signal & Image Processing : An International Journal(SIPIJ), Vol.1, No.2, December 2010

[6] Eugene T. Lin and Edward J. Delp, "A Review of Fragile Image Watermarks", Proceedings of the Multimedia and Security Workshop, 1999

[7] Jian-Guo Cao, James E. Fowler and Nicholas H. Younan, "An Image-Adaptive Watermark Based On A Redundant Wavelet Transform", Proceedings of the IEEE International Conference on Image Processing, , pp. 277-280 , Thessaloniki, Greece, October 2001

[8] Suhad Hajjara, Moussa Abdallah, Amjad Hudaib, "Digital Image Watermarking Using Localized Biorthogonal Wavelets", European Journal of Scientific Research, Vol.26, No.4 , pp.594-608, 2009

[9] Ersin ELBAS¸, "Robust multimedia watermarking: Hidden Markov model approach for video sequences", Turk J Elec Eng & Comp Sci, Vol.18, No.2, 2010

[10] Fındık, smail Baba and Erkan Ülker, "A digital robust image watermarking against desynchronization attacks", Scientific Research and Essays, Vol. 5, No.16, pp. 2288-2294, 18 August, 2010

[11] Sachin Goyal, Roopam Gupta, Ashish Bansal, "Application of Genetic Algorithm to Optimize Robustness and Fidelity of Watermarked Images", /International Journal on Computer Science and Engineering Vol.1, No.3, pp.239-242, 2009

[12] Jaseena K.U., Anita John, "An Invisible Zero Watermarking Algorithm using Combined Image and Text for Protecting Text Documents", International Journal on Computer Science and Engineering (IJCSE), Vol. 3, No. 6 , June 2011

[13] A.Essaouabi1, E.Ibnelhaj2,F.regragui, "Digital Image Watermarking for Arbitrarily Shaped Objects Based On SA-DWT", IJCSI International Journal of Computer Science , Vol. 5, 2009

[14] Aree Ali Mohammed, Haval Mohammed Sidqi, "Robust Image Watermarking Scheme Based on Wavelet Technique", International Journal of Computer Science and Security (IJCSS), Vol.5, No.4, 2011

[15] Sangeeta Jadhav, Anjali Bhalchandra, "Robust Digital Image-Adaptive Watermarking Using BSS Based Extraction Technique", International Journal of Image Processing (IJIP) , Vol.4, No. 1, pp77-88, 2010

[16] Todor Todorov, "Spread Spectrum Watermarking Technique for Information System Securing", International Journal of Information Theories & Applications, Vol.11, No.4, pp.405-408, 2004

[17] J.Samuel Manoharan, Kezi C.Vijila, A.Sathesh, "Performance Analysis of Spatial and Frequency Domain Multiple Data Embedding Techniques towards Geometric Attacks", International Journal of Security (IJS), Vol.4, No.3, 2009

[18] Mona M. Soliman, Aboul Ella Hassanien, Neveen I. Ghali and Hoda M. Onsi, "An adaptive Watermarking Approach for Medical Imaging Using Swarm Intelligent", International Journal of Smart Home, Vol. 6, No. 1, pp.37-50, January, 2012

[19] Umaamaheshvari and Thanushkodi, "High Performance and Effective Watermarking Scheme for Medical Images", European Journal of Scientific Research, Vol.67, No.2, pp. 283-293, 2012

[20] Sajjad Dadkhah, Azizah Abd Manaf and Somayeh Sadeghi, "Efficient Digital Image Authentication and Tamper Localization Technique Using 3Lsb Watermarking", International Journal of Computer Science , Vol. 9, No 2, January 2012

[21] Sujatha and Mohamed Sathik, "A Novel DWT Based Blind Watermarking for Image Authentication", International Journal of Network Security, Vol.14, No.4, PP.223-228, July 2012

[22] Amal Khalifa and Safwat Hamad, "A Robust Non-blind Algorithm for Watermarking Color Images using Multi-resolution Wavelet Decomposition", International Journal of Computer Applications, Vol.37, No.8, January 2012

[23] Mehmet Utku Celik, Gaurav Sharma, and A. Murat Tekalp, "Lossless Watermarking for Image Authentication: A New Framework and an Implementation", IEEE Transactions on Image Processing, Vol.15, No.4, pp.1042-1049, April 2006

[24] Mehmet Utku Celik, Gaurav Sharma and Murat Tekalp, "Lossless Watermarking for Image Authentication: A New Framework and an Implementation", IEEE Transactions on Image Processing, Vol. 15, No. 4, pp. 1042-1049, 2006