ISSN:0975-9646

A New Approach to Authenticate Images in Different Datasets Using a Lossless Image Watermarking Technique

[1]Arathi Chitla,[2] Dr. M. Chandra Mohan

[1]Associate Professor, Department of Computer Science & Engineering,
Telangana University, Nizamabad, Telangana State, India.
[2]Professor, Department of Computer Science & Engineering
JNTUH, Hyderabad, Telangana State, India.

Abstract- **With the tremendous expansion of the Internet and multimedia technologies in the recent past, digital media is being manipulated more frequently. Digital watermarking technologies are one of the best solutions for authentication and copyright protection of digital data. In this paper, we applied our lossless image authentication technique on different datasets, random images and also on different blocks of the same image. Our lossless watermarking technique achieved good comparative results than the existing watermarking techniques both in terms of authentication and also in terms of the perceptual quality.**

Keywords- **Authentication, Datasets, Lossless watermarking, Perceptual quality, Watermarking.**

I. Introduction

Exponentially growing passion of the people for the new information technologies is leading to the rapid growth of the multimedia document traffic (image, text, audio and video etc) in Internet. Nowadays, with the wide availability of many multimedia tools and some powerful image processing software, it is becoming difficult to determine whether an image is authentic or not. Image authentication systems can be classified in several ways according to whether they ensure strict integrity or content authentication, and also according to the storage mode of data authentication i.e. watermark or external signature. Many technologies were illustrated in the literature for image authentication. Digital watermarking techniques have been identified as one of the better alternate among them. Digital watermarking is a technique of embedding a digital code into a cover image without changing the image size or format and also keeping the visible quality and information of the image intact. Watermarking differs from steganography where any information which should be sent secretly can be hidden in a given host where as in watermarking, the embedded information known as watermark is related to the host image. Cryptography enhances the security of watermarking as an encrypted watermark is embedded instead of original watermark. .

Many watermarking techniques in the literature are achieving the authentication with the expense of image fidelity. But lossless recovery is important in many applications where there is a serious concern about image quality. Some examples include forensics, prepress industry, historical art imaging, medical and military applications. In these applications, images should be kept intact in any circumstances and before any operation they must be checked for integrity- that is the image has not been modified by non authorized people, and for authentication- that is the image belongs indeed to the correct sender [5]. Apart from authentication, the perceptual quality of the extracted image should be high which reflects the lossless recovery of the original image. Peak Signal to Noise Ratio (PSNR) penalizes the visibility of noise in an image. In many multimedia applications, any image with more than 30db is acceptable. But in the above applications where the quality of the data is often paramount, a PSNR around 50db is a definite indicator of quality image.

If the image is authentic, the distortion due to embedding process of watermarking can be completely removed from the original image after the watermark has been removed[1][2][3]. In this paper, we proposed one lossless watermarking method with that we authenticated images from FGNet face database, Google database, and random images and also we applied our technique on different blocks of the same image and compared the results to show the efficiency of our technique. The remaining portion of the paper is divided as follows. In section II, our proposed watermarking technique is presented. Application of our proposed technique on different datasets and experimental results are described in section III. Section IV includes the comparative analysis. And the conclusive remarks are presented in section V.

II. Proposed Watermarking Method

We propose a lossless image watermarking method where Elliptic Curve Cryptography (ECC) technique is used to authenticate original images by generating signed messages. The embedded data can be encrypted for enhanced security [7] ECC is a public key cryptography based on the mathematics of elliptic curves and uses the location of points on an elliptic curve to encrypt and decrypt information. After the authentication, the data embedding process is performed in which the computed information is inserted into the blocks of image data [6]. The data embedding process is accomplished by the wellknown Least Significant Bit (LSB) technique. Subsequently, the recovery and the verification processes are carried out to find out whether the extracted image is authenticated or not. We got good authentication results and PSNR values with this approach than conventional method [4].

We have improved the above process by introducing new decomposition technique called AQTD technique. Unlike the above technique where we used random decomposition to divide the image into blocks, here we employed AQDT for fragmenting the original image into five blocks and the signed communication from the ECC technique are implanted into the fifth block pixel values. Then the extraction and verification procedure are done to check the authenticity. This modified process overcomes the drawback of easy extraction of LSB embedding and enhanced the authentication and better perceptual transparency than previous and existing lossless watermarking techniques.

Fig1: Shows the structure of the proposed method

This process comprises of five stages namely, (i) Information (watermark) authentication by ECC, (ii) Image decomposition (iii) Watermark embedding on decomposed image, (iv) Information & image recovery, and (v) Image verification.

(i) Information (watermark) authentication by ECC- Here, we used prime field operations by choosing a prime number N , and finitely large numbers of basic points are generated on the elliptic curve between 0 to N . Then, we randomly select one basic point $p_i(x_i, y_i)$, a private key p_k <N and generate a public key $u_k = p_k * p_i$, signed message $s_m = (m_l, x_j, y_j), sg_l))$.

(ii) Image decomposition- The original image can be decomposed using Adaptive Quin Tree Decomposition method. In this technique, the image is divided into five blocks where each block has identical dimensions like width and length and the fifth block is positioned at the centre of the original image. We can estimate the fifth block with the help of mathematical equation. The central points of every block are evaluated and the intensity of first four blocks estimated with that of fifth block. The fifth block is transferred into the least intensity value block within a certain domain. Then the decomposition occurs in first four blocks. The procedure gets repeated till a certain threshold is arrived and z number of blocks are formed $z = 1,2,.........n$. The fifth block needs no decomposition, as it is the mixture of the upper left, upper right, lower left and lower right block.

(iii) Watermark embedding on decomposed image- Here the signed message is embedded into the image blocks by using the LSB method. Extract *n* number of pixels from every block by vertical raster scanning method. The corresponding binary values of the extracted n pixel are computed and the least significant bit values (LSB) from each pixel binary value are identified and are replaced by the signed message.

(iv) Information & image recovery- To recover the original image and message first divide the watermarked image into specified number of blocks and perform vertical raster scanning process on the image blocks based on the n value. Get n pixels LSB value from the blocks Divide this extracted LSB values into four parts with equal size. Compute the watermark to retrieve the original image.

(v) Image verification- The verification process is performed 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. If those two variables are equal then the image is authentic otherwise non authenticated image.

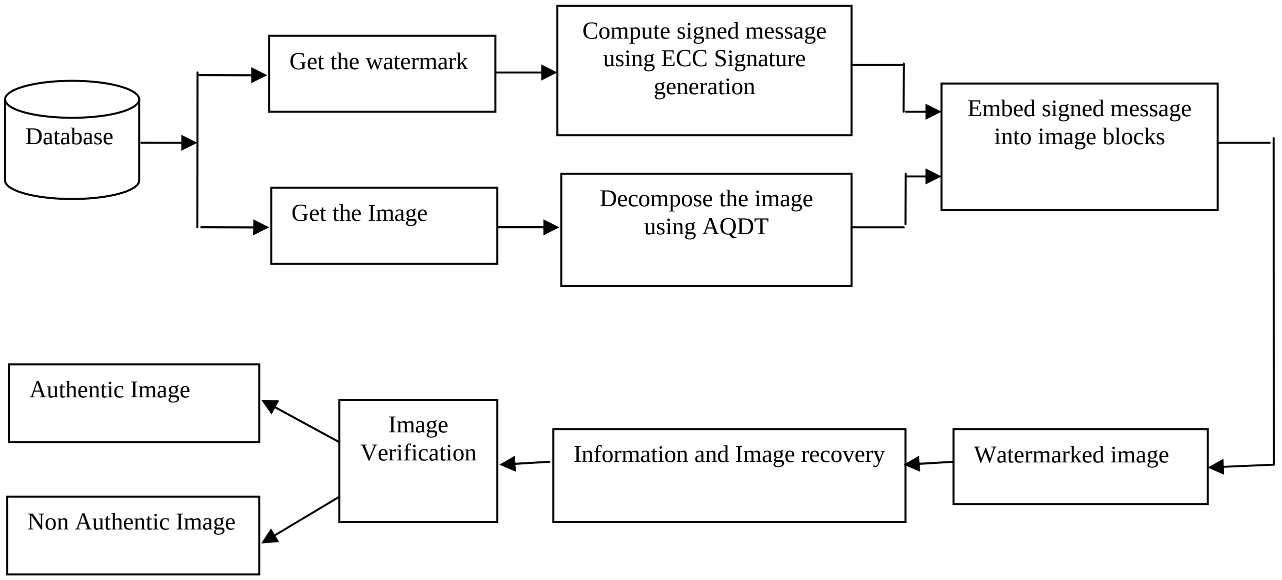

Database
Get the watermark
Compute signed message using ECC Signature generation
Get the Image
Decompose the image using AQDT
Embed signed message into image blocks
Watermarked image
Information and Image recovery
Image Verification
Authentic Image
Non Authentic Image

Fig1: Shows the structure of the proposed method

III. APPLICATIONS ON DIFFERENT DATASETS

We have taken images (Approximately 500 images) from FGNet face database, Google database, and random images and applied our watermarking technique on those images and sent to the destination. We applied our verification method at the destination on the retrieved image and identified the authenticity of that image. At the same time we also verified the perceptual quality of the retrieved image by calculating PSNR value of the retrieved image. We also verified the efficiency of our method by tampering the same images pretending that they have been sent from unknown person. We noted the verification result and PSNR value in this case too. Our method achieved 100% perfect verification results in this case with low Retrieved image PSNR values. Table1, Table2, Table3 and Table4 shows the results of different sample datasets when the watermark is “HLO” message.

Table 1: Proposed and improved method performance on sample FGNet face database

Table 2: Proposed and improved method performance on sample Google database

Table 3: Proposed and improved method performance on sample Random database

Table 4: Proposed and improved method performance on different blocks of same image

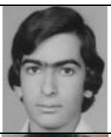
Message	Images from dataset	Retrieved image PSNR value (If the image sent from original sender) -Verification result		Retrieved image PSNR value (If the image sent from Unknown sender) -Verification result	
		Proposed method (Using ECC alone)	Improved method (ECC with AQTD)	Proposed method (Using ECC alone)	Improved method (ECC with AQTD)
HLO		75.0899-A	74.6647-NA	21.2771-NA	26.2922-NA
		73.8405-A	81.6716-A	20.3231-NA	26.4051-NA
		72.9511-A	79.6680-A	20.3134-A	26.3045-NA
		72.1459-A	78.8920-A	20.0555-A	26.2630-NA

Table 1: Proposed and improved method performance on sample FGNet face database

Message	Images from dataset	Retrieved image PSNR value (If the image sent from original sender) -Verification result		Retrieved image PSNR value (If the image sent from Unknown sender) -Verification result	
		Proposed method (Using ECC alone)	Improved method (ECC with AQTD)	Proposed method (Using ECC alone)	Improved method (ECC with AQTD)
HLO		75.5038-A	81.3820-A	24.0268-NA	30.3281-NA
		74.7120-A	80.2750-A	21.4900-NA	27.3526-NA
		74.3644-A	79.7635-A	20.8833-NA	25.9985-NA
		72.0143-A	78.4423-A	22.9665-NA	27.8701-NA

Table 2 : Proposed and improved method performance on sample Google database

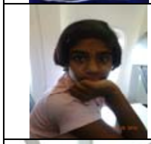
Message	Images from dataset	Retrieved image PSNR value (If the image sent from original sender) -Verification result		Retrieved image PSNR value (If the image sent from Unknown sender) -Verification result	
		Proposed method (Using ECC alone)	Improved method (ECC with AQTD)	Proposed method (Using ECC alone)	Improved method (ECC with AQTD)
HLO		68.15-A	70.83-A	19.96-NA	19.95-NA
		68.07-A	70.78-A	20.67-A	20.66-NA
		67.28-A	69.52-A	20.22-NA	20.20-NA
		67.17-A	69.48-A	21.52-A	21.49-NA

Table 3 : Proposed and improved method performance on sample Random database

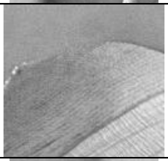
Message	Images from dataset	Retrieved image PSNR value (If the image sent from original sender) -Verification result		Retrieved image PSNR value (If the image sent from Unknown sender) - Verification result	
		Proposed method (Using ECC alone)	Improved method (ECC with AQTD)	Proposed method (Using ECC alone)	Improved method (ECC with AQTD)
HLO		68.8137-A	74.2273-A	19.9117-NA	26.1839-NA
		67.6743-A	75.6137-A	20.2391-NA	27.3442-NA
		67.7708-A	75.4320-A	20.8829-NA	26.1700-NA
		67.3747-A	75.7266-A	20.8589-NA	26.3302-A
		67.4875-A	76.8017-A	19.9112-NA	26.2288-NA

Table 4 : Proposed and improved method performance on different blocks of same image

IV. COMPARATIVE ANALYSIS

Here we compared our two methods performance on different datasets and image blocks in Fig1. The figure shows the efficiency of our methods clearly

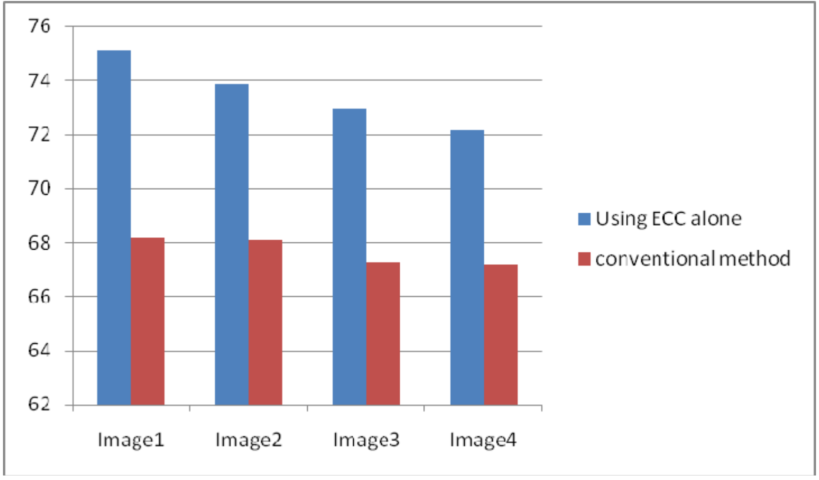


Fig2: Comparison of Proposed and Conventional LWM Image Authentication Techniques in Terms of their PSNR values (images from original sender)

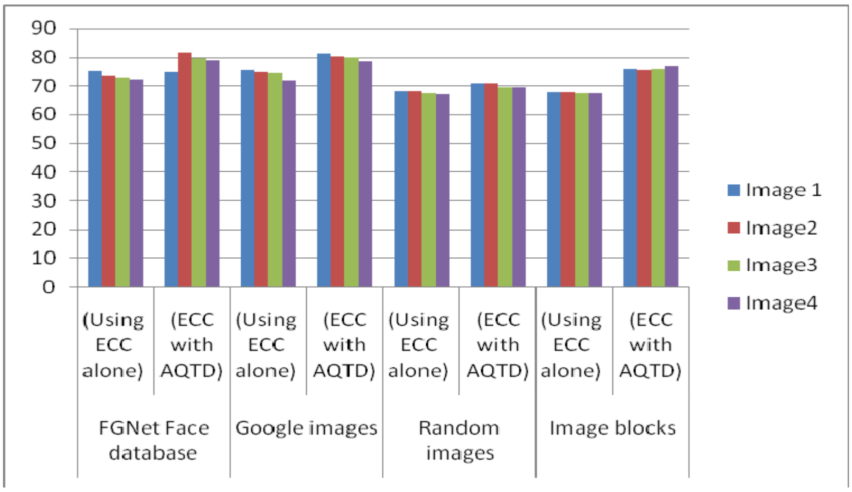


Fig3: Comparison of proposed and improved method performance in terms of Retrieved image PSNR values on different datasets on the sample images if the image sent from the original sender

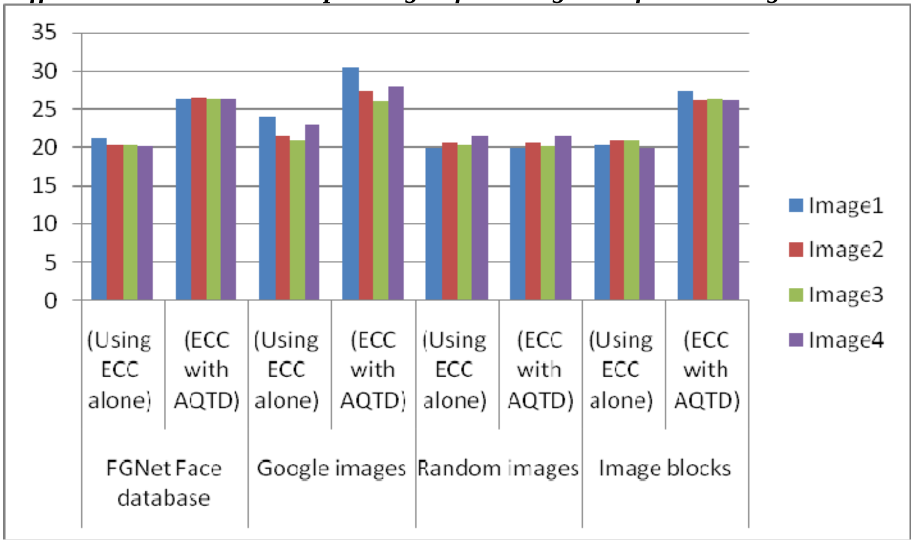


Fig4: Comparison of proposed and improved method performance in terms of Retrieved image PSNR values on different datasets on the sample images if the image sent from the unknown sender

Sno	Dataset Name	Original sender (No.of authentications out of 4)		Unknown sender (No. of Non authentications out of 4)	
		ECC alone	ECC with AQTD	ECC alone	ECC with AQTD
1	FGNet Face Database	4	3	2	4
2	Google Images	4	4	4	4
3	Random Images	4	4	2	4
4	Image Blocks	4	4	4	3

Table 5: Comparative results of correct authentications both in case of original sender and Unknown sender

The above table depicts the authentication capabilities of our methods. If the images are sent from the original sender, our both method exhibits approximately equal performance, where as if the image sent from unknown sender, our improved method (ECC with AQTD) gave better authentication results than our first method.

V. Conclusion

We proposed two lossless watermarking methods to authenticate an Image by combining cryptography with spatial domain semi fragile digital watermarking techniques where watermark is embedded in the image pixels to authenticate digital images losslessly. We made use of Elliptic Curve Cryptography to generate signature to the embedding watermark. In one method, the embedding process was done using LSB technique. We have divided the image into blocks and embedded the signed watermark on each block of the image. In order to strengthen the LSB approach, we introduced one effective decomposition technique called Adaptive Quin Tree Decomposition technique in our second method with which it will become difficult to identify the block where the watermark was embedded. We got good results in our first method compared to the existing methods. We got even better results in our second approach compared to our first approach and also with the existing methods.

References

[1] J.Fridrich, M. Goljan and R.Du “Invertible Authentication” Proc. SPIE Conf. Security and Watermarking of Multimedia Contents III, Vol. 4314, 2001, Pg. 197-208

[2] Jeng- Shyang Pan, Hao Luo and Zhe-Ming Lu “ A Lossless Watermarking Scheme for Halftone Image Authentication” , IJCSCN International Journal of Computer Science and Network Security, Vol.16, No.2B, Feb 2006, Pg:147-151

[3] Sang-Kwang Lee, Young-Ho Suh and Yo-Sung Ho; “Reversible Image Authentication Based on Watermarking”; ICME 2006, IEEE,pg: 1321-1324

[4] Mehmet Utku Celik,Gaurav Sharma and A.Murat Teklap; “Lossless Watermarking for Image Authentication: A New Framework and an Implementation”;In IEEE Transactions on Image Processing, volume 15, No 4,April 2006, pages 1042-1049.

[5] Samia Boucherkha and Mohamed Benmohamed ;“A Lossless Watermarking Based Authentication System for Medical Images”;In WASET; Volume 1,January 2005,pages 100-103

[6] Chih-Chin Lai; “An Improved SVD-based watermarking scheme using human visual charecteristics”Optics Communications 284 (2011) Elsevier, pages 938-944

[7] Nithin Nagaraj and Rakesh Mullick; “Zero-distortion lossless data embedding”;SPIE USE; Volume 1,2004