A SIMPLE SYSTEM TO INTEGRATE IMAGE PROTECTION AND AUTHENTICATION

K.Alice[1], N.Ramaraj[2], N.Kanimozhi[3]

[1, 3] Department of CSE, GKM College of Engineering and Technology, Chennai
[2] Department of EEE, Vignan's University, Guntur

ABSTRACT

In this paper, we propose a system that protects and authenticates digital image by applying Data Hiding schemes in Cipher text images. Image features are extracted using Zernike moments which acts as embedded data and used for authentication purposes. The image is preprocessed by employing a Histogram shrink operation and then Encrypted using Paillier cryptosystems. To this cipher text image, features extracted are embedded using Multilayer Wet Paper coding. At the receiver, the image is decrypted and original image along with embedded data are recovered. To this received image Zernike moment's features are extracted and compared with the received feature data to verify the authenticity of the image. The proposed system simultaneously authenticates and provides security for the digital image.

I. INTRODUCTION

In recent days, digital images have widespread use in multimedia data. With the enormous image editing application the security and integrity of images are greatly challenged. The images may also be vulnerable to many attacks during transmission over public or wireless channels. Such attacks in image data could change the decision when digital images are used as evidence in criminal investigation, medical images, forensic sciences, notary documents etc.

To ensure image authenticity, content based authentication greatly reduces the computation than strict authentication. The content of the image is represented as a small code called Hash code [1]. Hash code can be generated by extracting local and global features [2], Watermarking methods [3] [4], Transform co-efficient [5] [6], and much more. In recent work combining two or more hashed techniques to generate the hash code is also most common to take advantage of different hashing techniques [7]. The main drawback of representation of image by its content is the possibility of having some feature vector for different images [7]. This vulnerability can be removed decisively, but can be avoided by generating features based on local and global image features. Thus for ensuring authenticity of image hash code based on feature of image can better be used. Moments are set of values used to describe the information content in the image. A proper subset of moments is always the best choice that describes the exact content of image. Zernike moments have an orthogonal basis functions and are used as image features in most authentication system [2].

The most traditional way of providing security to any type of data in cryptosystem. Image encryption is used in many applications for providing security. Paillier cryptosystem algorithm [8] is used for Image encryption. To take advantage of Protection and authentication the proposed system embeds the hash code with the encrypted image. For embedding, the data into the cipher text image multilayer wet paper coding is used.

The remainder of the paper is organized as follows: Section II Paillier cryptosystem, Section III Zernike Moments, Section IV Overview of wet paper coding, Section V Implementation of the proposed system, Section VI Experimental Results and Section VII Concludes the paper.

II. PAILLIER CRYPTOSYSTEM

Select two large prime numbers p and q and calculate n = p.q such that λ = lcm (p-1, q-1) where lcm means the Least common multiple and gcd (n, (p-1) . (q-1)) = 1 where gcd means the Greatest common divisor.

The pair <n,g> in $Z_{n^2}^*$ act as public key and the pair <λλλλ , μ> act as private key where

$$\mu = (L(g^{\lambda} \bmod n^2))^{-1} \bmod n \quad \text{where } L(x) = \frac{x-1}{n}$$

Cipher text

c(i , j) =$[g^{m(i,j)} .(r(i,j))^n]$ mod n^2 where r(i , j) is a random integer in Z_n^*

Plain text

m(i , j) = $L((c(i\ ,j))^{\lambda}$ mod $n^2).\mu\ mod\ n.$

III. ZERNIKE MOMENTS

The Complex Zernike moments of order n with repetition m for a continuous image function f(x,y) for X Y image plane are defined as

A_{nm}=n+1/π $\iint_{x^2+y^2<=1}$ f(x, y) V_{nm}* (P, θ) dx dy
A_{nm}=n+1/π $\int_0^2$ π $\int_0^{1f}$ (P, θ) R_{nm}* (P) exp (-jmo) P.dP.dθ

Where n is either positive integer of 0.m takes positive and negative integer with the constants n-|m|= even and |m|<=n, P is the length of the vector from the origin to the pixel at (X, Y) and θ is the angle between vector P and the X-Axis is the counter clockwise direction.
The Zernike Polynomial is given as

V_{nm}(x, Y) = V_{nm} (P sinθ, P cosθ) = R_{nm} (P) exp (jmθ)

It refers complex conjugate.The features of invariance under image rotation makes Zernike function of the most important moments.

IV. MULTILAYER WET PAPER CODING

In encrypted image, cipher text pixels are divided into two sets. Set A including C(i , j) with odd values of (i + j). Set B including C(i , j) with even values of (i + j).

Without any loss in data, the pixel number in Set A is $\frac{N}{2}$. It employs Error correction codes to expand the additional data as a bit sequence with length $\frac{N}{2}$, and maps the $\frac{N}{2}$ bits in the coded bit sequence to the cipher text pixel in Set A in a one to one manner.

When Paillier Cryptosystem is used, if the bit is 0 the corresponding cipher text pixel is modified as $C'(i\ ,j) = C(i\ ,j).\,g^{n-\delta}.\,(r'(i\ ,j))^n mod\ n^2$ where r' (i , j) is a randomly selected integer in Z_n^*. If the bit is 1, the corresponding cipher text pixel is modified as $C'(i\ ,j) = C(i\ ,j).\,g^{\delta}.\,(r'(i\ ,j))^n mod\ n^2$.

This way an encrypted image containing additional data is produced. Additional data are embedded into Set A. Set B will be used for data extraction since the pixel values in Set A are difficult to be precisely obtained on receiver side. It leads to possible errors in directly extracted data.

Therefore the error correction coding mechanism is employed here to ensure successful data extraction and perfect image recovery.

V. IMPLEMENTATION

The architecture of the proposed system is as shown in figure. In the sender side the input image undergoes a preprocessing stage. In the Preprocessing the input image of size 512 X 512 is converted to grayscale image. For this grayscale image Zernike moments of order n = 10 is calculated and hash code [H_S] is generated. The same grayscale image is then converted to Image Histogram and encrypted using Paillier cryptosystem. To this cipher text hash code generated using Zernike moments is embedded using Multilayer wet paper coding algorithm and is transmitted.

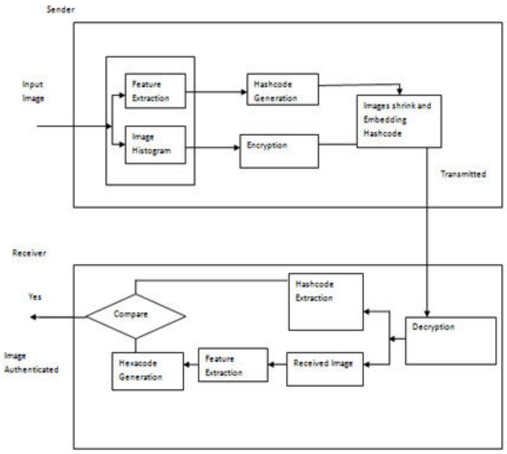


Figure 1-Architecture diagram

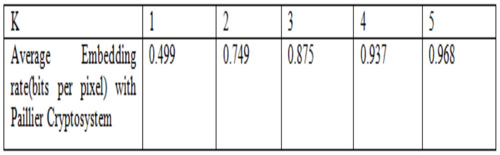
In the receiver side, the received image is decrypted and the hash code [H_S] and Image is extracted. To this extracted image again Zernike Moments of order n = 10 is calculated and hash code is generated [H_R]. Now H_S and H_R is compared using Correlation co-efficient and authenticated if it is above certain threshold τ.

VI. EXPERIMENTAL RESULTS

The size of the image is taken as 512 X 512. A median filter is applied to eliminate noise and is converted to grayscale image. For this grayscale image Zernike moments ‘Z’ of order n = 10 is extracted and is normalized using a random vector R using ZM = [Z + R mod 256]. This ZM now becomes the code to be embedded. The grayscale image converted to Image Histogram and is encrypted using Paillier Cryptosystem. The obtained cipher text is then divided into two set A and B and the set is shrinked to half to embed the hash code ZM in bit 0 and bit 1 of each pixel. A and B is combined to get transmitted image.

Table-1 list the average value of embedding rates when K - LSB planes are used for carrying the additional data in 50 encrypted images.

TABLE.1- Average Embedding Bit Rate



K	1	2	3	4	5
Average Embedding rate(bits per pixel) with Paillier Cryptosystem	0.499	0.749	0.875	0.937	0.968

The performance of the system is measured using peak signal to noise ratio for various embedding rates. For an image of size M x N the MSE and PSNR are given as

$$MSE = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j-1}^{N}((f_{max}(x_i,y_j)-(f(x_i,y_j)))^{2}$$

$$PSNR = 10 * log_{10}(\frac{2^n-1}{MSE})$$

VII. CONCLUSION

This paper proposes a system that integrates image protection and security. Due to the compatibility of data embedding and encryption, the required performance of the system is 100% achievable. However on the receiver side there is slight distortion introduced in decrypted image due to the presence of additional data embedded in the cipher text image during the transmission.

REFERENCES

[1] A.Haouzia, R Noumeir,”Methods for image authentication A survey” , Multimedia tools Appl 39: 1-46,Springer 2008.

[2]Lima Sebatian,Abraham Varghese,Manesh.T ,” Image Authentication by content preserving robust image hashing using local and global features”,1877-0509, published by Elsevier B.V, Copyright 2015

[3] Tri.H.Nguyen,Duc.M.Duong and Duc.A.Doung, ”Robust and High Capacity watermarking for image based on DWT-SVD”, IEEE RIVF, International conference on computing and communication Vision for Future(RIVF) 2015.

[4] F. Khelifi and J.Jiang Technologies Research Innovation and, “perceptual image hashing based on virtual watermark detection,”IEEEtrans. Image process. vol. 19, no. 4, pp. 981-994, Apr.2010

[5] Yang,H.Z.Shu, G.N.Han, C.Toumoulin, L.M.Luo, “Efficient Legendre moment computation for grey level images” Laboratory of Image Science and Technology, Department of Biology and Medical Engineering , Southeast University, 210096, 2014.

[6] Y. Lei, Y. Wang, and J. Huang, “Robust image hash in radon transform domain for authentication,” Signal process. : Image commun.Vol 26, no. 6, pp. 28[8] A. Fouad and J. Jianmin, “Analysis of the security of perceptual image hashing based on non-negative matrix factorization, “IEEE Signal process. Lett. , vol. 17, no. 1, pp. 43-46, Jan. 2010.

[7] K.Alice, N.Ramaraj, “Combining Hashing Techniques in Image Authentication System : A survey”, International Journal of scientific research,Vol 4 Issue 10 October 2015 ISSN 2277-8179

[8] Xinpeng Zhang,Jing Long,Zichi Wang,Hang Cheng,”Lossless and Reversible data hiding in Encrypted images with public key cryptography”,IEEE transactions on Circuit and Systems for vodeo Technology Vol.26,No.9.Sep 2016

[9] A.Swaminathan, Y. Mao, and m. Wu, “Robust and secure image hashing,” IEEE Trans. Inf. Forensics security, vol, 1, no. 2, pp. 215-230,Jan. 2006.