Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 115 (2017) 423–430

Procedia Computer Science

www.elsevier.com/locate/procedia

An Efficient Watermarking Technique for Biometric Images

G. Dinesh Kumar*, Dontoju Pranay Teja, Sykam Sreekar Reddy, N. Sasikaladevi

Department of Computer Science and Engineering,
School of Computing, SASTRA University, Thanjavur, TN, India

Abstract

This paper provides a good way of digital watermarking framework using biometric image as watermark by the application of homomorphic encryption system. Thus, it provides data confidentiality and also authenticity. Here, the biometric image is watermarked inside the standard benchmark images. The robustness of the watermarks in the image are verified through measurement of Peak Signal-to-noise ratio (PSNR), Correlation coefficient (CC%), and noise test. The biometric images are obtained by subtracting watermarked images with benchmark images.

© 2017 The Authors. Published by Elsevier B.V.
Peer-review under responsibility of the scientific committee of the 7th International Conference on Advances in Computing & Communications.

Keywords: Biometric Image; Watermarking; Homomorphic encryption; Homomorphic decryption; Compression

1. Introduction

Digital watermarking is a technique that embeds digital information inside a carrier signal. Recently, Watermarking has been an active area of research. These watermarks can be used to verify the authenticity or integrity of the carrier signal or can be used to show the identity of its owner. The images can be stored in cloud based storages. Here the privacy has to be taken into account. Thus, the image is encrypted using homomorphic encryption scheme and can be accessed by intended persons by decrypting it using homomorphic decryption scheme. Now, Homomorphic cryptosystem has been widely used all over the public cloud. In homomorphic cryptosystem, the user can perform operations on the encrypted data without decrypting the data and get the same result as performed on the original data. Thus, it maintains confidentiality over the cloud based storages.

This paper is organized as follows, Firstly, related work specifies the research regarding digital watermarking,

*Department of Computer Science and Engineering, School of Computing, SASTRA University, Thanjavur, Tamilnadu
dineshkumardinu16@gmail.com

1877-0509 © 2017 The Authors. Published by Elsevier B.V.
Peer-review under responsibility of the scientific committee of the 7th International Conference on Advances in Computing & Communications
10.1016/j.procs.2017.09.101

image compression, cloud challenges,homomorphic encryption that was done earlier and the proof shows us about the emerging cryptography usage in data integrity and cloud storage security. Secondly, the proposed model clear picture about the proposed method of image encryption and the sample results are shown. Finally, result and analysis shows that in order to provide the efficiency of our work key space analysis, key sensitivity analysis, Histogram analysis, PSNR analysis, MSE analysis, correlation analysis, Noise analysis are performed.

2. Related Work

Watermarking are also used for providing security for securely storing medical images inside the image of the patient. To maintain the confidentiality and reduce the mishandling of the patient data, Double Watermarking of PET images using patient ID and ECG signal is proposed [1]. The efficient homomorphic encryption is proposed and it allows to perform calculations on the data stored by encrypting it. The efficiency of homomorphic property of the algorithm is analysed [2]. The Image compression algorithm using 2D wavelet transform[9] provides a way of compressing the image. The analysis of any work tells us the efficiency of the designed model.The Key space analysis , Key sensitivity analysis, time analysis , Peak signal to noise ratio , Mean square error analysis , Correlation co-efficient analysis are used in the image encryption scheme[3].An image histogram illustrates how pixels in an image are distributed by graphing the number of pixels.Analysis was done earlier and presented us that for any plain image,the cipher image should be in sucha a way that it should generate a uniform histogram[4].Key sensitivity analysis and histogram analysis are performed to check the efficiency of the existing algorithms[5].Correlation analysis[6] and PSNR & MSE analysis[7] are considered to be more prominent for image encryption.Based on this study, we are proceeding our work on security of medical images using Homomorphic Encryption scheme.

3. Proposed Framework

The proposed methodology watermarks a benchmark image with a biometric image using homomorphic scheme. This contains encryption and decryption phase. Fig 1 shows the framework of the methodology.

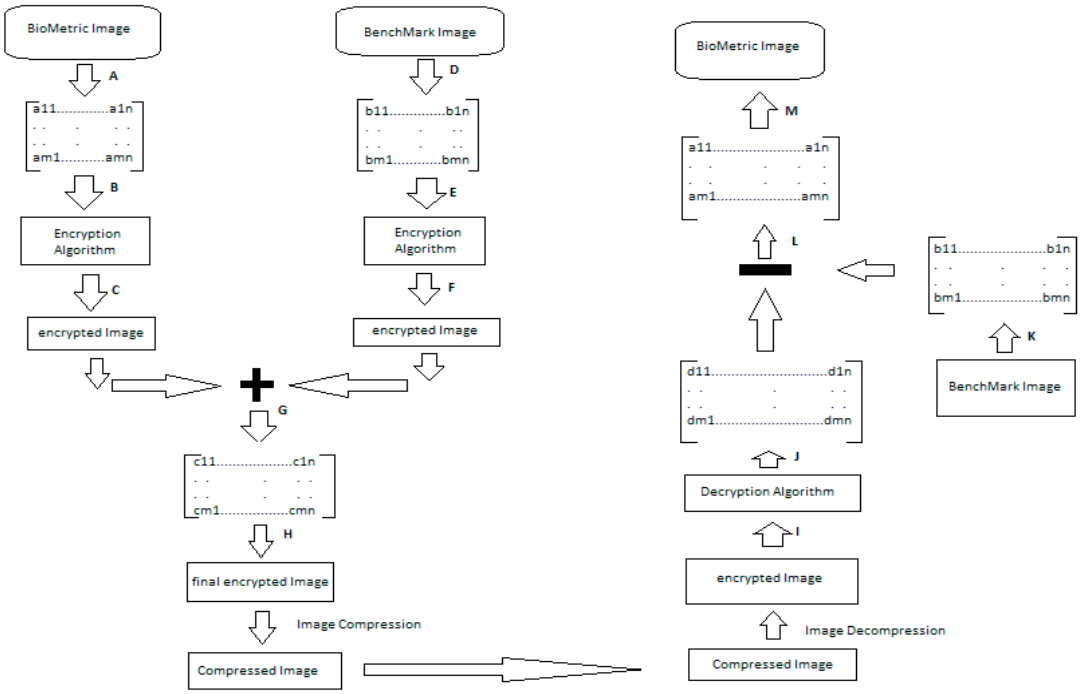


Fig 1. Biometric Image Watermarking Framework

A - Input Image1 (Biometric image) is rasterized and matrix is obtained.
B - Matrix of Input Image1 is sent to Homomorphic Encryption Algorithm.
C - Encrypted Image of Input Image1(Biometric Image) is obtained.
D - Input Image 2 (Benchmark Image) is rasterized and matrix is obtained.
E - Matrix of Input Image 2 is sent to Homomorphic Encryption Algorithm.
F - Encrypted Image of Input Image2(Benchmark Image) is obtained.
G - Resultant encrypted matrix is obtained by adding two images (Biometric and Benchmark).
H - Encrypted Image formed by the resultant matrix.
Image Compression - Encrypted Image is compressed using Wavelet Transform.

Image Decompression - Compressed image is decompressed using Inverse Wavelet Transform.
I - Encrypted image is sent to Homomorphic decryption algorithm.
J - Decrypted matrix is obtained.
K - Benchmark image is rasterized and matrix is obtained.
L - Subtract the bench mark image from Decrypted image to form original Input matrix.
M - Original image (Biometric Image) is formed from the obtained matrix.

3.1 Key Generation Algorithm

It is based on probabilistic algorithm for key generation.

Table 1: Parameters for key generation Algorithm

Parameter	Type	Constraints
P	Big prime	Public
Q	Big prime	p>>q
Z	Random no.	Set of integers under p

This algorithm takes security parameter λ as an input and produces sk as output
Input: security parameter (λ)
Output: sk (Secret key) and p (public parameter) sk←(z, q), Keygen (λ)→(sk, p)

3.2 Encryption algorithm

This is probabilistic algorithm which takes **sk** (Secret key) and **a** (plain text) and **d** (cipher text degree) as an input and produces **c** (cipher text) as an output
Input: sk (secret key), a (plain text), d (cipher text degree)
Output: c (cipher text)

E (sk, a, d) → c

We choose a Big random number **w** such that(|w|+|q|<|p|), where |w| denotes bit length of w

$$\mathbf{E\ (sk, a, d) = z^{d}\ (w * q + a)\ mod\ p}$$

3.3 Decryption algorithm

This is deterministic algorithm which takes **c** (cipher text), **d** (cipher text degree), **sk** (secret key) as an input and produces **a** (plain text) as an output
Input: c (cipher text), d (cipher text degree), sk (secret key)
Output: a (plain text)
D (sk, c, d) → a

$$\mathbf{D\ (sk, c, d) \rightarrow (c \times z^{-d}\ mod\ p)\ mod\ q}$$

$\mathbf{z^{-d}}$is multiplicative inverse of $\mathbf{z^{d}}$ in the field Fp.

3.4 Properties of Homomorphic Encryption

Let c_1, c_2 be the cipher texts of two plaintexts a_1, a_2 with two big primes p and q where p>>q and d_1, d_2 be cipher texts degree of c_1c_2 and w_1, w_2 are big random integers

Then we have $c1=z^{d1}(w_1q+a_1)$

$c_2=z^{d2}(w_{2q}+a_2)$

Homomorphic Addition:

$(c_1+c_2) \bmod p = z^{d1} (w_1q+a_1) \bmod p + z^{d2} (w_2q+a_2) \bmod p$

$z^{d1} ((w_1+ w_2) q+a_1+a_2) \bmod p$ if $d_1 = d_2$

condition: $((w_1+ w_2) q+a_1+a_2) < p$

Homomorphicsubtraction:

$(c_1-c_2) \bmod p = z^{d1}(w_1q+a_1) \bmod p - z^{d2}(w_2q+a_2) \bmod p$

$z^{d1}((w_1- w_2) q+a_1-a_2) \bmod p$ if $d_1=d_2$

condition: $((w_1-w_2) q+a_1+a_2) <p$

Homomorphic multiplication:

$(c_1\times c_2) \bmod p= z^{d1}(w_1q+a_1) \bmod p \times z^{d2} (w_2q+a_2) \bmod p$

$z^{d1+d2}(w_1w_2q^2+w_1qa_2+w_2a_1q+a_1\times a_2) \bmod p$

$z^{d1+d2}((w_1w_2q+w_1a_2+w_2a_1) q+a_1\times a_2) \bmod p$

condition: $|w_1|+|w_2|+2|q|+1<|p|$

Thus, we can perform all operations directly on cipher texts without decrypting the message and can be stored for further usage.

4. Results and Analysis

The proposed algorithm adds the biometric image as a watermark in the benchmark image. The following are the results of the above algorithm.

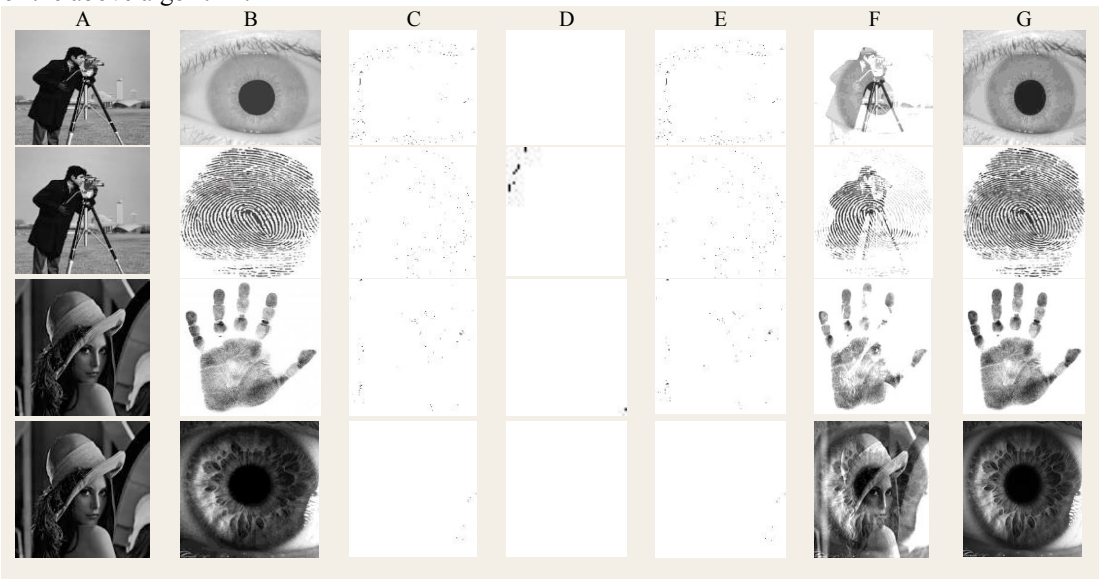


Fig 2: Watermarked Images and Separated Images. A – Benchmark Image, B – Biometric Image, C – Encrypted Watermark Image, D – Compressed Image, E – Decompressed Image, F – Decrypted Watermark Image, G – Biometric Image obtained from the watermarked Image.

In order to measure the efficiency of encryption and compression process various test analysis are to be performed. The following test analysis are performed.

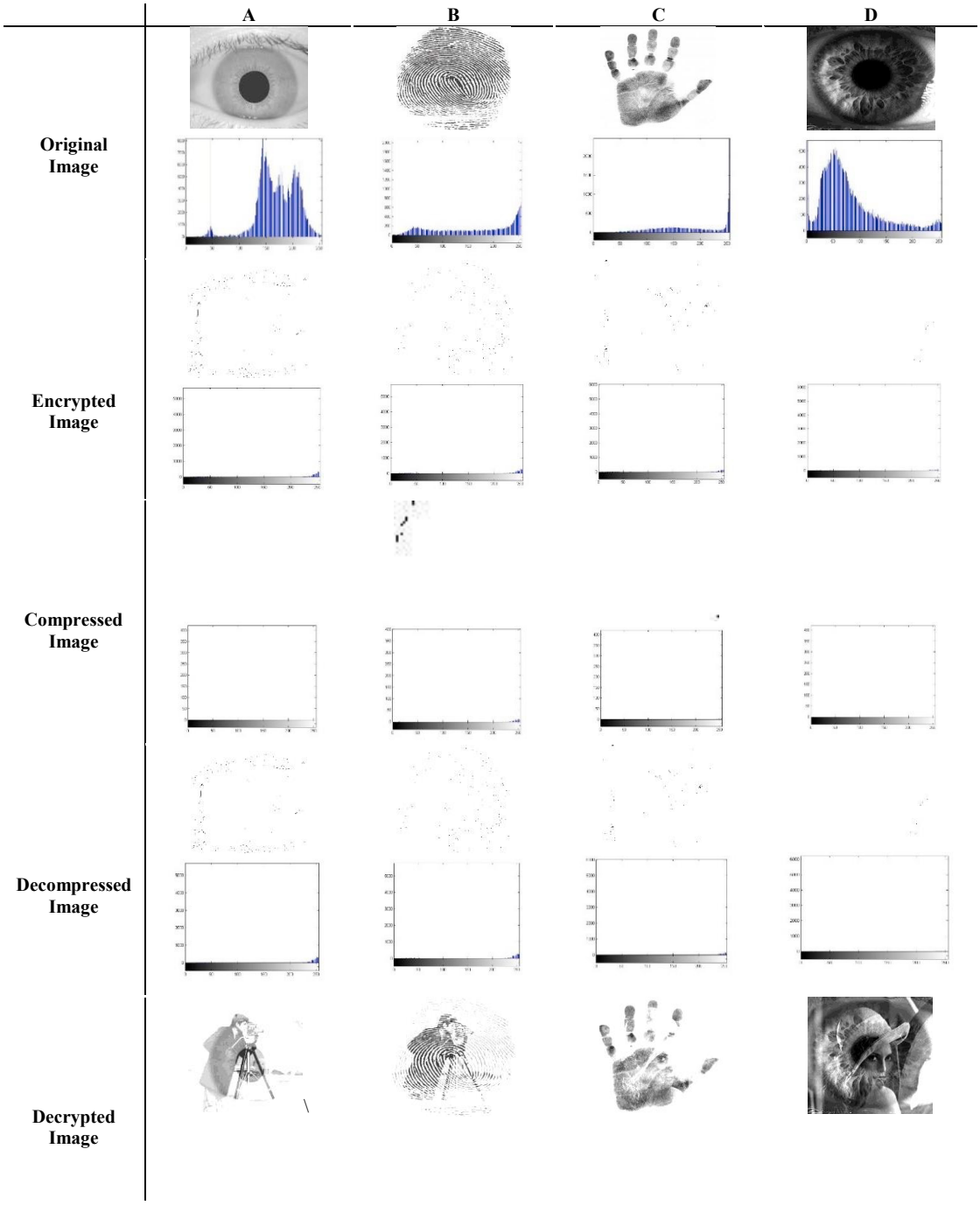
4.1 Key Space Analysis

Key space analysis is a concept which specifies the range of number of bits need to be used for a secret key. Key with more number of bits (long key) results in reduction of execution speed and a key with less number of bits (short

key) will make attacks easier for intruders. In order to provide more security key space should be $< 2^{100}$.

4.2 Histogram Analysis

A Histogram is a graphical representation of color distribution over the image. The horizontal axis represents color variations and vertical axis represents number of pixels.



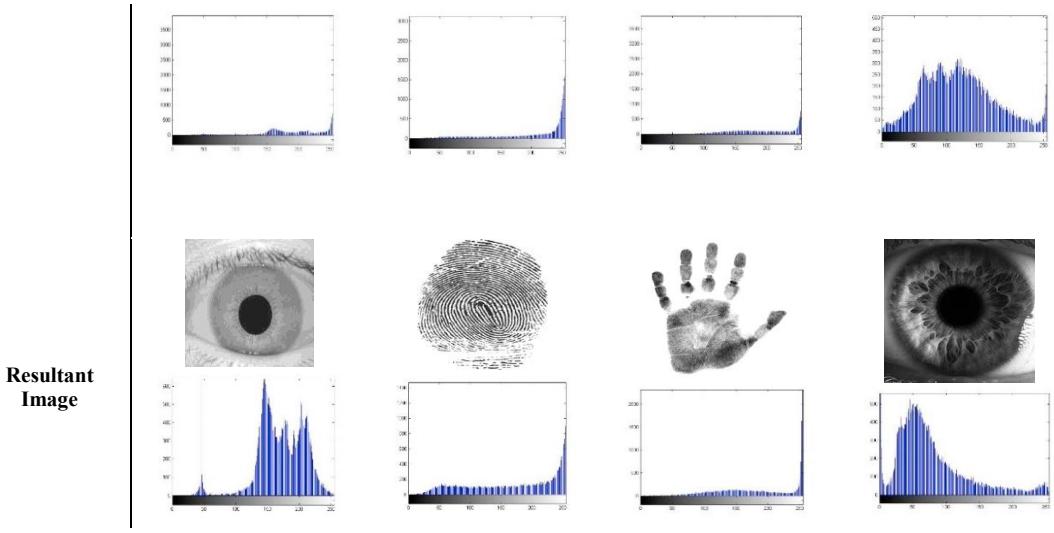


Fig 3: Histogram Analysis of Biometric Images. A – Eye image, B – FingerPrint Image, C – PalmPrint Image, D – Iris Image

4.3 Correlation Analysis

Correlation analysis refers to the strength of relationship between two or more variables. Correlation coefficient lies between the range of -1 to 1. The value of -1 represents perfectly negative correlation which means as the value of one variable increases the other decreases. value of 0 indicates perfect positive correlation which means as one value increases same does the other. The value of 0 represents there is no relationship between variables.

A B C D

Fig 4: Images taken for correlation analyis

Here 10,000 pairs of horizontal, vertical, diagonal random pixels are selected and correlation analysis is performed. Correlation coefficient (r) is given by the formula below

$$r= \frac{N\Sigma xy-(\Sigma x)(\Sigma y)}{\sqrt{\sqrt{[N\Sigma x^2-(\Sigma x)^2][N\Sigma y^2-(\Sigma y)^2]}}}$$

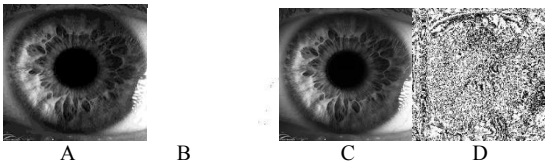
Where N=number of pairs of scores, Σxy=sum of the products of paired scores,Σx =sum of x scores, Σy =sum of y scores, Σx^2 =sum of squared x score, Σy^2 =sum of squared y scores

Table 2: Correlation between two adjacent pixels in the original, encrypted and decrypted Image

Image	Horizontal			Vertical			Diagonal		
	Original	Encrypted	Decrypted	Original	Encrypted	Decrypted	Original	Encrypted	Decrypted
A	0.9791	0.3270	0.9786	0.9861	0.2993	0.9861	0.9730	0.2475	0.9696
B	0.7524	0.1643	0.7539	0.5806	0.1494	0.5840	0.5687	0.1324	0.5768
C	0.9705	0.2864	0.9705	0.9692	0.4057	0.9704	0.9516	0.2630	0.9513
D	0.9798	0.2154	0.9785	0.9770	0.2756	0.9773	0.9625	0.1264	0.9614

4.4 Key Sensitivity Analysis

It states that algorithm should be sensitive for small change in the Input parameter (i.e. even single bit change in input parameter should lead to false result). The proposed method satisfies the above condition even for one bit change of key value the image resulted is incorrect. As 1 bit of LSB of key change will result in mean square error of original image and decrypted image.



A B C D

Fig 5: A-Medical Image, B-Encrypted Image of Image Obtained by adding bench mark and Biometric Image, C-Decrypted Image formed by subtracting the bench mark image from combined decrypted Image, D-Decrypted Image formed by changing one bit of key.

4.5 PSNR and MSE Analysis

Peak signal to noise ratio(PSNR) is the ratio between maximum possible power of a signal to possible power of corrupting noise.

$$\text{PSNR}=20 * log \frac{255^2}{\sqrt{MSE}}$$

Table 3: PSNR Values for Biometric Images

Biometric Image	PSNR(Orig-Enc)	PSNR(Orig-Dec)
A	-115.2043	Infinity
B	-115.2187	Infinity
C	-115.0635	Infinity
D	-115.1647	Infinity

MSE: Mean square error is the average of squares of the errors or deviations

$$\text{MSE}=\frac{1}{N*M}\sum_{n=1}^{N}\sum_{m=1}^{M}[f1(i,j)-f2(i,j)^2]$$

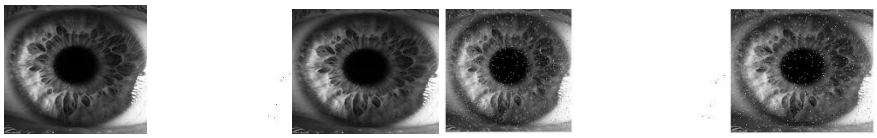
Where f1 and f2 are intensitiy functions of decrypted and original image. N*M is the size of image

Table 4: MSE Values for Biometric Images

Biometric Image	MSE(Orig-Enc)	MSE(Orig-Dec)
A	$3.3146e^{+11}$	0
B	$3.3256e^{+11}$	0
C	$3.2089\ e^{+11}$	0
D	$3.2845e^{+11}$	0

4.6 Noise Test Analysis

In order to measure the robustness of algorithm against noise we perform Noise Test Analysis. Here we have added salt and pepper noise to Medical Image.



A B C D E F

Fig 6: Noise Test Analysis of Biometric Image. A-Original Medical Image, B-Encrypted Image of Image Obtained by adding bench mark and Medical Image, C-Decrypted Image formed by subtracting the bench mark image from combined decrypted Image, D-The Image formed by adding salt and pepper noise to original image, E-Encrypted Image of D, F-Decrypted Image.

5. Conclusion

In this paper, we proposed a novel digital watermarking technique with a homomorphic cryptosystem.Biometric images should be used for providing authentication and should be secured in the cloud. At the same time it should pave the way for performing certain operations in a secured way. The analysis that we have made proves that our work will provide efficient security to biometric images for transferring and storing securely.

References

[1] Mohammad-Saleh Nambakhsh, Alireza Ahmadian, Habib Zaidi. A Contextual based double watermarking of PET images by patient ID and ECG signal. *Elsevier* 2011; 104:418-425;

[2] Lichun Li, Rongxing Lu, Kim-Kwang Raymond Choo, Anwitaman Datta, Jun Shao. Privacy-Preserving-Outsourced Association Rule Mining on Vertically Partitioned Databases. *IEEE Transactions on Information Forensics and Security* 2016; 11:1847-1861.

[3] Narendra K Pareek. Design and Analysis of a Novel Digital Encryption Scheme. *International Journal of Network Security and Its Application* Issue-2 2012; 4:95-108.

[4] Li Li, Ahmed A. Abd El-Latif,XiamuNiu. Elliptic Curve Elgamal Based Homomorphic Image Encryption Scheme for Sharing Secret Images. *Elsevier* 2012; 92:1069-1078;

[5] Weijja Cao, Yicong Zhou, C.L Philip Chen, Liming Xia. Medical image Encryption Using Edge Maps. *Signal Processing – Elsevier* 2016; 132:96-109.

[6] Sara Tedmori, Nijad Al Najdawi. Image Cryptographic algorithm based on the Haar wavelet transform. *Information Sciences-Elsevier* 2014; 269:21-34

[7] Pinki, Rajesh Mehra. Estimation of the image quality under different distortion. *International journal of Engineering and Computer Science* 2016; 5:17291-17296.

[8] M.-S. Hsieh, D.-C. Tseng, Y. -H. Huang. Hiding digital watermarks using multiresolution wavelet transform. *IEEE Transaction Ind. Electron* 2001; 48:875-882.

[9] A.S. Lewis, G. Knowles, Image Compression using the 2D wavelet transform. *IEEE Transaction on Image Processing 1(2)* 1992; 244-250.

[10] Jasni M Zain, Abdul R M Fauzi. Medical Image Watermarking with Tamper Detection and Recovery. *IEEE/EMBS Annual International Conference* 2006; p. 3