ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Secure Image Processing Using Discrete Wavelet Transform And Paillier Cryptosystem

Kanithi Sri Ramulu
MTech Scholar
Department of CSE
Miracle Educational Society
Bhogapuram-535216, A.P, India

Mrs A.Gauthami Latha, M.Tech,
Associate Professor
Department of CSE
Miracle Educational Society
Bhogapuram-535216, A.P, India

Abstract:

Cryptosystems play an important role in secure image processing, but not all cryptosystems are appropriate for secure image processing. The reason is that most cryptosystems, such as data encryption standard (DES) and advanced encryption standard (AES), do not retain the algebraic relations among the plaintexts after encryption. A special kind of cryptosystems, the Homomorphic cryptosystems, is able to keep the algebraic structure of the plaintext after encryption, and thus is particularly suitable for this purpose. So we propose a frame work for performing DWT/IDWT and encryption/decryption by using paillier cryptosystem. Taking a 2-D Haar wavelet transform as an example, we conduct a few experiments to demonstrate the advantages of our method in secure image processing. We also provide computational complexity analyses and comparisons. This process reducing memory usage and time for the entire process.

Keywords: Cryptosystems, advanced encryption standard, Homomorphic cryptosystems, image processin.

INTRODUCTION

Image processing technology in the encrypted domain provides powerful tools to make secure implementation possible. Image processing in the encrypted domain, also referred to as secure image processing, and has attracted considerable attention in recent years. This new technology may promise one kind of application in future. In the case when the owners and manipulators of data are two different parties. For example, in the scenario of network media distribution, the customer may be asked to embed a watermark in the media to trace illegal copies. Since plain media can be easily attacked by the customer during watermarking, a solution is to embed the watermark in the encrypted media, whose content is protected by the cryptosystems. Cryptosystems play an important role in secure image processing, but not all cryptosystems are appropriate for image processing in the encrypted domain. The reason is that most cryptosystems, such as data encryption standard and advanced encryption standard, do not retain the algebraic relations among the plaintexts after encryption. A special kind of cryptosystem, the homomorphic cryptosystem, is able to keep the algebraic structure of the plaintext, and thus is particularly suitable for this purpose.

This is a desirable feature in modern communication system architectures. Homomorphic encryption would allow the chaining together of different services without exposing the data to each of those services, for example a chain of different services from different companies could 1) calculate the tax 2) the currency exchange rate 3) shipping, on a transaction without exposing the unencrypted data to each of those services. Homomorphic encryption schemes are malleable by design. The homomorphic property of various cryptosystems can be used to create secure voting systems, collision-resistant hash functions, private information retrieval schemes and enable widespread use of cloud computing by ensuring the confidentiality of processed data.

The existing homomorphic cryptosystems can be divided into two categories, partially homomorphic

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

cryptosystems and fully homomorphic cryptosystems. Partially homomorphic cryptosystems keep only one algebraic structure of the plaintexts, such as the Paillier cryptosystem [1], while fully homomorphic cryptosystems permit to compute additions and multiplications homomorphically, allowing the computation of any polynomials in the encrypted domain. For example, Gentry's fully homomorphic encryption scheme [2] works on binary values, which corresponds to the computation of any logical circuits.

DWT is a commonly used mathematical tool in signal processing. With different wavelet bases and decomposition levels, DWT can extract different kinds of information from digital media, and is therefore likely to be carried out in the encrypted domain. DWT in the encrypted domain is expected to be used as a building block in various applications, for example, secure media watermarking, secure feature extraction and secure information retrieval. Firstly, we describe a framework for performing DWT and IDWT in homomorphic encrypted domain. The framework can be used for general purpose operations on encrypted data. A Walsh- Hadamard transform-based image watermarking scheme was proposed in [3], possesses the character of blind watermark extraction, in both the decrypted domain and the encrypted domain. which For instance, pyramid algorithms can be implemented in the encrypted domain by using our strategy. We then conduct the analysis of data expansion for decomposition and reconstruction. Secondly, we propose a method, called the multiplicative inverse method (MIM), to remove the quantization factor The proposed method provides a solution to the problem of data expansion. with much less data expansion.

Paillier Cryptosystem

The Paillier cryptosystem, named after and invented by Pascal Paillier in 1999, is a probabilistic asymmetric algorithm for public key cryptography. Homomorphic encryption is a form of encryption which allows specific types of computations to be carried out on cipher text and generate an encrypted result which, when decrypted, matches the result of operations performed on the plaintext.

Specifically, there exist two algebraic operations corresponding to each other, one in plaintext space and the other in ciphertext space. If $m1$ and $m2$ are any two plaintexts in homomorphic cryptosystems, we have $D[E[m1] \circ E[m2]] = m1 <> m2$ where $D[\cdot]$ and $E[\cdot]$ are the decrypting and encrypting operators, respectively. Operators "$\circ$" and "<>" perform the corresponding algebraic operations in the ciphertext and the plaintext spaces, respectively.

Related Work:

The availability of image processing algorithms that work directly on the encrypted data would be of great help for application scenarios where "valuable" image information must be produced, processed, or exchanged in digital format. Z. Erkin, A. Piva, S. Katzenbeisser [4] proposes that, new class of signal processing techniques operating in the encrypted domain as signal processing in the encrypted domain. Signal processing in the encrypted domain, combined with cryptographic protocols [5] can provide an effective solution to this problem. In this proposed system focus on signal processing in the encrypted domain without considering the cryptographic protocols. Cryptosystems play an important role in secure signal processing, but not all cryptosystems are appropriate for signal processing in the encrypted domain. The reason is that most cryptosystems, DES, AES do not retain the algebraic relations among the plaintexts after encryption.

A special kind of cryptosystems, the homomorphic cryptosystems, is able to keep the algebraic structure of the plaintext, and thus is particularly suitable for this purpose. Partially homomorphic cryptosystems keep only one algebraic structure of the plaintexts, such as the ElGamal cryptosystem [9], the Paillier cryptosystem [6]. There have been some related works on signal processing in the encrypted domain over the past few years. Bianchi *et al*. [7] conducted an

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

investigation on the implementation of the discrete Fourier transform (DFT) as well as the fast Fourier transform (FFT) on encrypted signals. A Walsh-Hadamard transform based image watermarking scheme was proposed in [3], possesses the character of blind watermark extraction, in both the decrypted domain and the encrypted domain. In [8], Erkin *et al*. proposed a privacy-preserving face recognition system based on the Paillier cryptosystem.

DWT [14] is a commonly used mathematical tool in signal processing. With different wavelet bases and decomposition levels, DWT can extract different kinds of information from digital media, and is therefore likely to be carried out in the encrypted domain. DWT in the encrypted domain is expected to be used as a building block in various applications, for example, secure media watermarking, secure feature extraction and secure information retrieval.

In the Peijia Zheng and Jiwu Huang [11-12] describe a framework for performing DWT and IDWT in homomorphic encrypted domain. The framework can be used for general purpose operations on encrypted data. For instance, pyramid algorithms can be implemented in the encrypted domain by using our strategy. We then conduct the analysis of data expansion and derive an upper bound on the accumulated error for decomposition and reconstruction. Secondly, propose a method, called the multiplicative inverse method (MIM), to remove the quantization factor without decryption. The proposed method provides a solution to the problem of data expansion.

Existing system:

In the existing system we have developed a frame work for applying dwt /idwt on the encrypted image. In this process dwt is applied on the encrypted image .But encrypted image contains mostly real values. So integer coefficients can be obtained by quantizing *hd* and *gd* . By this process the data expansion is occur .MIM method is applied before decryption.

Disadvantages:

1. By applying above process, data expansion has occurred. It consumes more memory.
2. By applying DWT/IDWT/MIM it takes more time for execution.

Proposed system:

For overcome the above problems we proposed a new frame work for dwt/idwt .we firstly applied dwt on the input image then it gives four sub band images those are 1. Approximation coefficients 2.horizontal 3.vertical 4.diagonal coefficients. Approximation coefficients contain required information for reconstructing the original image. All detailed coefficients are maximum zeros and approximately those values near to zero. So, on the approximation coefficients we have applied paillier encryption algorithm .Then decrypt the encrypted image by using paillier decryption algorithm. Then reconstruct the image by applying idwt on the decrypted image .By applying dwt on the input image we could not multiply with any scaling factor, because input image pixel values are integer values.

Advantages:

1. We can reduce the memory usage by applying encryption on approximation coefficients.
2. We can reduce time by eliminating the method MIM, scaling factor.

Proposed Algorithm

Homomorphic encryption is a form of encryption which allows specific types of computations to be carried out on ciphertext and generate an encrypted result which, when decrypted, matches the result of operations performed on the plaintext.

Key Generation

step 1. Choose two large prime numbers P and Q randomly and independently of each other.
step 2. Compute N=PQ and $\lambda = \text{lcm}(P-1, Q-1)$.
step 3. Select random integer g where $G \in Z*_{N^2}$
step 4. The public (encryption) key is (N, G) .

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The private (decryption) key is(λ).

Encryption

Let $M \in Z_N$ be a plaintext. The encryption process of m can be described as

- $E [M, R] = G^M R^N \bmod N^2 = C.$

Where $R \in Z^*_N$ is an integer chosen at random. According to the Paillier cryptosystem the ciphertext c is in $Z^*_{N^2}$.

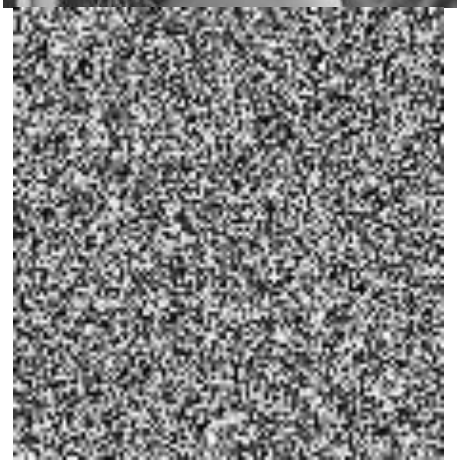

Fig.Input Image

Fig. Encrypted Image

Decryption

Let $C \in Z*_{N^2}$ be the ciphertext.

The decryption process of c can be described as

$D [C] = (L (C^{\lambda} \bmod N^2) / L (G^{\lambda} \bmod N^2)) \bmod N,$

Where L (·) denotes the function

$L (U) = \frac{U - 1}{N}$

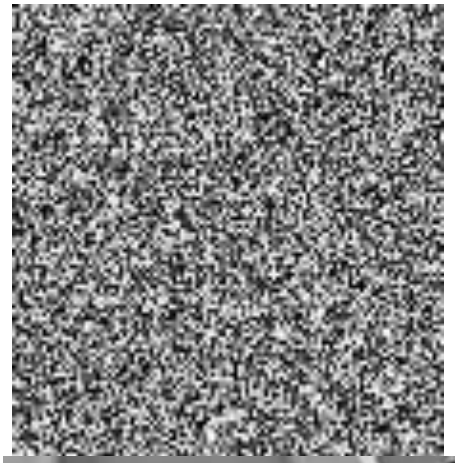

Fig.Encrypted image

Fig.Decrypted image

The following equations show some useful homomorphic properties of the Paillier cryptosystem

$D [E [M1, R1] E [M2, R2]] \bmod N^2 = M1 + M2 \bmod N .$

$D [E [M, R]]^K \bmod N^2 = K \cdot M \bmod N$

$\forall K \in Z_N.$

Existing system Architecture:

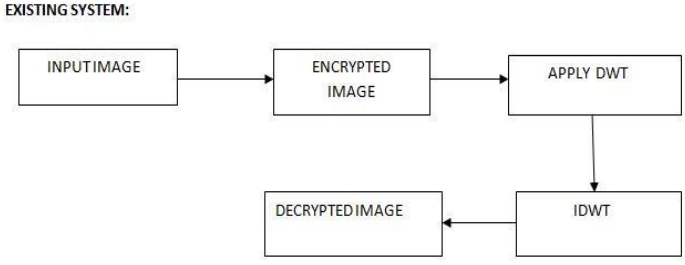

Fig.Existing System Architecture

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Proposed System Architecture:

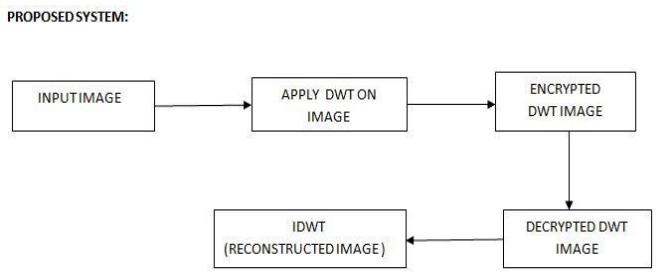

Fig.Proposed System Architecture

SCREEN SHOTS

Without MIM

Reconstructed image

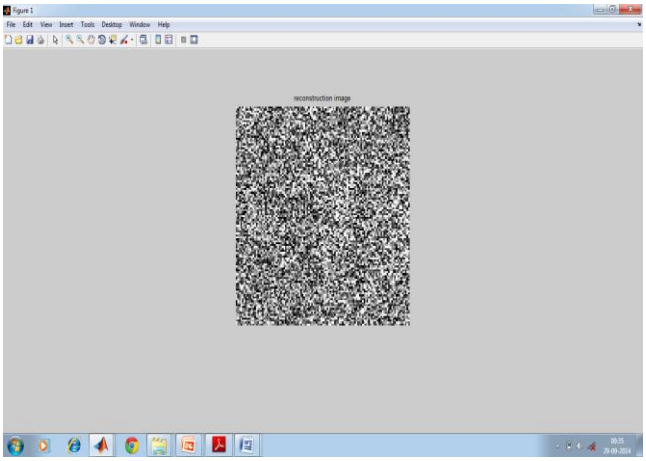

Fig.Reconstructed image

Decrypted image

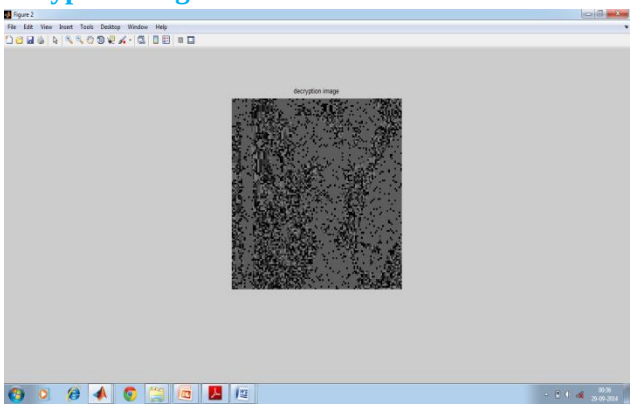

Fig.Decrypted image

With MIM method

Reconstructed image

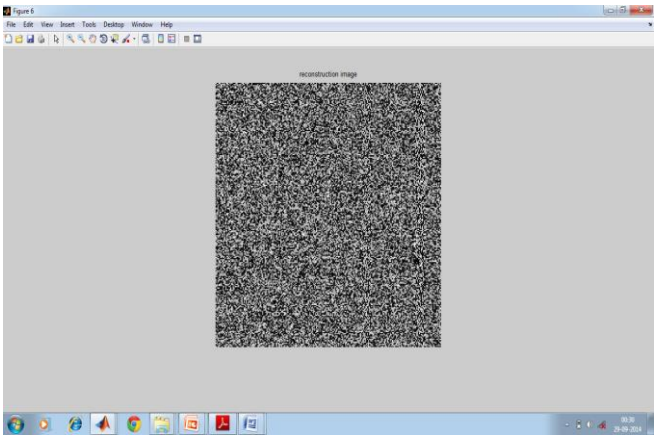

Fig.Reconstructed Image

Decrypted image

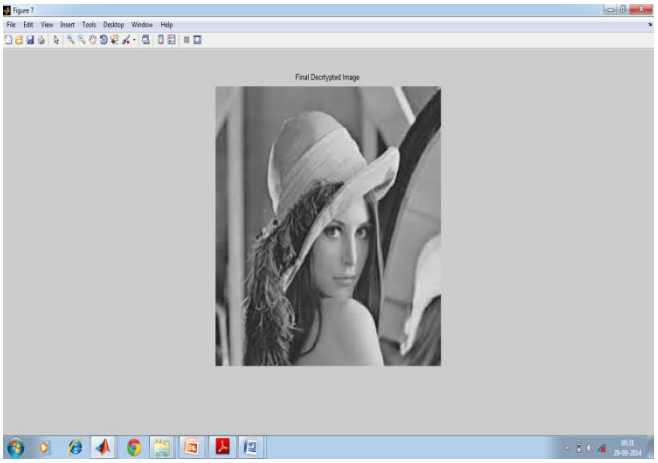

Fig. Final Decrypted Image

With proposed Method

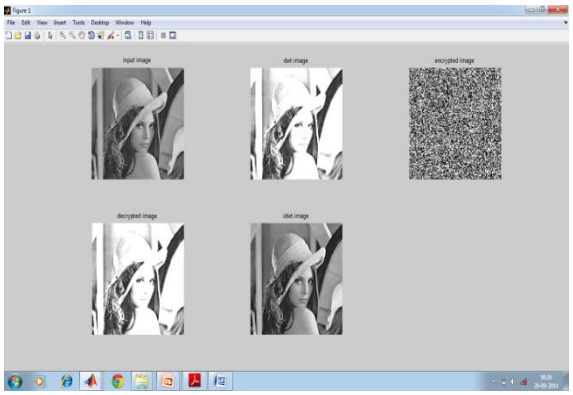

Fig.Proposed method results

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

CONCLUSION

In the proposed implementation of DWT and IDWT in a homomorphic encrypted domain and tackled the problem of data expansion caused by quantization. The main contributions are listed as follows.

- We have proposed a framework to implement DWT and IDWT in the encrypted domain by using homomorphic properties.
- We have investigated 2D Haar wavelet transform in our experiments. The experiment results demonstrate the validity of our framework and the advantages of the proposed method.
- Standard images with various details are used to test the efficiency of the proposed work.
- An experimental result such as quality assessment shows that the decrypted image is identical with the original image without any loss of data. Various security and statistical analysis techniques shows that the proposed algorithm is secured. By this proposed algorithm it reduces execution time and memory usage.

References

[1] Peijia Zheng, Student Member, IEEE, and Jiwu Huang, Senior Member, IEEE, Discrete Wavelet Transform and Data Expansion Reduction in Homomorphic Encrypted Domain, IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 22, NO. 6, JUNE 2013

[2] C. Gentry, "Fully homomorphic encryption using ideal lattices," in Proc. 41st Annu. ACM Symp. Theory Comput., 2009, pp. 169–178.

[3] P. Zheng and J. Huang, "Walsh- Hadamard transform in the homomorphic encrypted domain and its application in image watermarking," in Proc. 14th Inf. Hiding Conf., 2012, pp. 240–254.

[4] A. Yao, "Protocols for secure computations," in Proc. 23rd Annu. Symp. Foundations Computer Science, 1982, pp. 160–164.

[5] P. Paillier, "Public-key cryptosystems based on composite degree residuosity classes," in Proc. Adv. Cryptology, 1999, pp. 223–238.

[6] T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," IEEE Trans. Inf. Forensics Security, vol. 4, no. 1, pp. 86–97, Mar. 2009.

[7] Z. Erkin, M. Franz, J. Guajardo, S. Katzenbeisser, I. Lagendijk, and T. Toft, "Privacy-preserving face recognition," in Proc. 9th Int. Symp. Privacy Enhanc. Technol., 2009, pp. 235–253.

[8] Z. Erkin, A. Piva, S. Katzenbeisser, R. Lagendijk, J. Shokrollahi, G. Neven, and M. Barni, "Protection and retrieval of encrypted multimedia content: When cryptography meets signal processing," EURASIP J. Inf. Security, vol. 2007, pp. 1–20, Jan. 2007.

[9] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Trans. Inf. Theory, vol. 31, no. 4, pp. 469–472, Jul. 1985.

[10] R.Asha & M.Raja babu, Discrete Wavelet Transform Based Steganography for Transmitting Images, IJMETMR, http://www.ijmetmr.com/oldecember2014/RAsha-MRajababu-108.pdf, Volume No: 1(2014), Issue No: 12 (December)

[11] N.HABEEP1, R.Dayal Raj2 "Homomorphic encrypted domain with DWT methods" ISSN (Online): 2348 – 3539, ISSN (Print): 2348 – 3431,2014

[12] P. Zheng and J. Huang, "Implementation of the discrete wavelet transform and multi resolution analysis in the encrypted domain," in Proc.19th ACM Int. Conf. Multimedia, 2011, pp. 413–422.

[13] T. Bianchi, S. Turchi, A. Piva, R. Labati, V. Piuri, and F. Scotti, "Implementing fingercode-based identity matching in the encrypted domain," in Proc. IEEE Workshop

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Biometric Meas. Syst. Security Med. Appl., Taranto, Italy, Sep. 2010, pp. 15–21.

[14] I. Daubechies, Ten Lectures on Wavelets. Philadelphia, PA, USA: SIAM, 2004.

[15] S. Goldwasser and S. Micali, "Probabilistic encryption," J. Comput. Syst. Sci., vol. 28, no. 2, pp. 270–299, 1984.

[16] Munish Rattan, Ravi Kumar Research scholler "Analysis Of Various Quality Metrics for Medical Image Processing" Volume 2, Issue 11, November 2012.