International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 10 | October - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

Image Encryption in Transform Domain Employing DWT and Chaos

Iram[1] Prof. Pankaj Raghuwanshi[2]

Abstract: Off late conventional image data hiding and encryption mechanisms have seen a shift towards homomorphic images which can be thought of being created from a constant illumination and a varying reflectance. In this proposed work, the Fresnel Transform is employed to convert normal images into homomorphic images to reduce the redundancy of images. Subsequently, the image is converted to the transform domain using the 4th level Discrete Wavelet Transform. The truncation of the DWT is done at the 4th level so as to limit the complexity of the system. Once the image is converted to the transform domain, it is encrypted using the Chaotic Baker Map. The embedded data can be extracted from the encrypted domain itself without the mandatory necessity of first decrypting the image thereby making the secret image extraction faster and less perceptible. The evaluation of the proposed technique is done based on the histogram analysis, the MSE, PSNR, Correlation and Entropy. It has been shown that the proposed system performs better compared to the previously existing technique in terms of the PSNR for the same image from the benchmark USC-SIPI image dataset.

Keywords: Data Hiding, Homomorphic Images, Fresnel Transform, Discrete Wavelet Transform, Chaotic Baker Maps, PSNR

I. INTRODUCTION

Encryption is a very important concept in the area of Image security and Cryptography. Encryption is the process of encoding data in a secured form that is only meant for the authenticated receiver and can be decrypted only by the intended user. It serves to preserve the integrity and confidentiality of the image data. The process involves converting the original data into cipher text by utilizing high end algorithms for encryption. It is a very important process that's helps in protecting the data from intruders [3]. The websites use encryption methods to transfer and share data. The stronger the encryption system, the better it is to protect it from adversaries and third party intruders. The image encryption can help in preserving the image data and make it more safe and secure.

Fig. 1 Image Encryption vs. Image Data Hiding

Image Hiding is another important concept that is necessary. It can help in areas where encryption is not successful. With image hiding the data can be completely hidden and shade in hidden form. Some major features of data hiding include imperceptibility which refers to the data being unrecognizable and hidden. Another feature is the capacity to embed the

data of the image. The next feature is the security of the image [4]-[5]. The image security must be robust and strong. Hence image security is an important paradigm in the security of images

III. PROPOSED METHODOLOGY

Homomorphic images are images which can be thought of being created from a constant illumination and a varying reflectance [1]. They are becoming very popular for image and video security with more advanced graphic processing units (GPUs) being developed. Mathematically:

$$I = f\Pi(\Psi, R) \quad (1)$$

Here,
I is the original image
Ψ is the illumination
R is the reflectance
Π represents the constant product operator
f represents a function of.

Typically, the constant illumination component and the high pass components can be separated using filters. A low pass filter is used to separate the illumination component and a high pass filter is used to separate the reflectance component.

The image intensity of such an image is given by:

$$I(x,y) = i(x,y).r(x,y) \quad (2)$$

Here,
I is the image intensity which is a function of the coordinates (x,y)
(x,y) are the pixel coordinates
i is the illumination function
r is the reflectance function
Taking log on both sides:

$$\log[I(x,y)] = \log[i(x,y)] + \log[r(x,y)] \quad (3)$$

In general, the illumination component is similar in value for most images and generally have a lot of redundancy or redundant data.

The reflectance however varies significantly for different images. Thus to avoid redundancy in the encrypted image, save space and reduce the size of the image, only the reflected component can be encrypted [26]-[27]. In the LSB positions of the encrypted data, the illumination co-efficient can be embedded. The embedded data can later extracted from the LSB locations and the complete image can be recreated [28]-[30].

The technique to convert normal images to homomorphic images is the Fresnel Transform which is mathematically given by:

For an image I(x,y),

$$F(x2,y2) = \iint_{-\infty}^{+\infty} I(x1,y1) \exp\left[-\frac{j\pi}{\delta}.\{(x2-x1)^2 + (y2-y1)^2\}\right] dx1dy1 \quad (4)$$

Here,
F is the image in the Fresnel Domain
x,y are the co-ordinates
I is the original image
δ is the Transform parameter given by:

$$\delta = \lambda d \quad (5)$$

Here,
λ is the wavelength
d is the separation between the image and the Fresnel plane

The Fresnel transform is also given by the convolution integral of the image I(x1,y1) and the term $\exp\left[-\frac{j\pi}{\delta}.\{(x2-x1)^2 + (y2-y1)^2\}\right]$ which is also called the propagator function (p)

Thus, the Fresnel transform can thus be computed as:

$$F(x,y) = conv(\{I(x,y) * p\} \quad (6)$$

Here,
conv represents the convolution operation
$*$ represents the convolution operator.

Without loss of generality, the convolution of any two functions g and h is given by:

$$conv(g,h) = \int_{-\infty}^{+\infty} g(\tau)h(t-\tau)d\tau \quad (7)$$

Here,
τ is called the translator variable

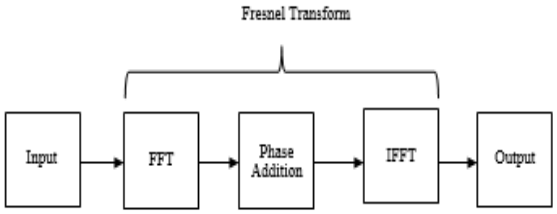

Fig.2 Computation of Fresnel Transform using Fourier Method

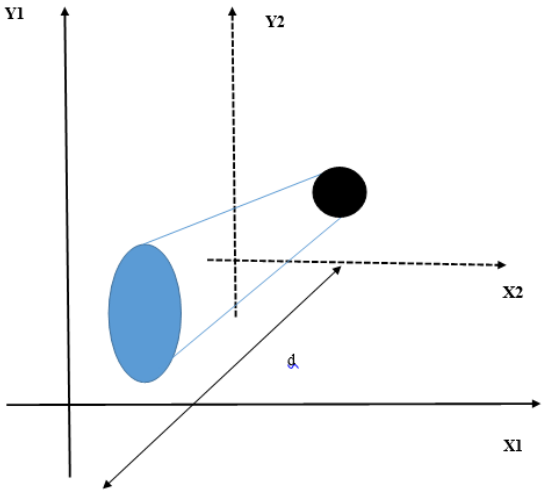

Fig.3 The Graphical Illustration of the Fresnel Transform

The discrete wavelet transform is a complex invertible transform which is useful for the analysis of data which are highly variable and show lack of smoothness or continuity such as images. The Wavelet Transform is mathematically defined as:

The DWT of a sequence $\psi(n)_{j,k}$ is:

$$S(n)=\frac{1}{\sqrt{M}}[\sum_k W\Phi(Jo,k)\,\Phi(n)_{jo,k}+\sum_{j=jo}^{\infty}\sum_k W\psi(j,k)\,\psi(n)_{j,k} \quad (8)$$

The Scaling function is given by:

$$W\Phi(Jo,k)=\frac{1}{\sqrt{M}}\sum_n S(n).\Phi(n)_{jo,k} \quad (9)$$

The Wavelet Function is given by:

$$W\psi(j,k)=\frac{1}{\sqrt{M}}\sum_n S(n).\psi(n)_{j,k} \quad (10)$$

Where $\frac{1}{\sqrt{M}}$ Is Normalizing term

with n=0, 1,2,……..M-1,

The DWT renders two co-efficient values which are the approximate co-efficient (CA) and detailed co-efficient (CD). The approximate co-efficient contains the maximum spectral information while the detailed co-efficient contains the details and is generally affected by noise effects the most.

After the image is converted to the transform domain using the discrete wavelet transform, it is encrypted using the Chaotic Baker Map (CBM technique). The chaotic Baker map is an effective tool which encrypts images based on an mxm data size permutation. The benefit of the chaotic baker map is the fact that it is extremely sensitive to changes in the initial conditions. A slight change in the initial conditions makes the output of the Baker Map change to an exceedingly large level thereby exhibiting the property of chaos.

For digital images, the Dicretized Baker Map is used in which every stream of bits which has a length 'k' is the CBM vector with the property that each of the elements in stream divides m perfectly. Mathematically,

$$for\ [v_1, v_2 \ldots\ldots\ldots v_n] \in B \quad (11)$$

$$M\%B_i = 0 \quad (12)$$

Here,

B_i represents each element of the Baker Vector B.

For encrypting an mxm of the image, the following transformation is made:

$$B_v(l.s) = [\frac{M}{v_i}(l - M_i) + s.mod\left(\frac{M}{v_i}\right), \frac{v_i}{M}\{s - s.mod\left(\frac{M}{v_i}\right)\} + M_i] \quad (13)$$

The following constraints should be met for the above transformation

$$M_i \le l < l < +M_i + v_i \quad (14)$$

And

$$0 \le s < M \quad (15)$$

The Chaotic Baker Map (CBM) has an important property of bijective association wherein each pixel element of the plain text image is associated invertible manner to a unique element of the cipher text image in a one to one correspondence.

The flowchart of the proposed system is depicted in figure 4.

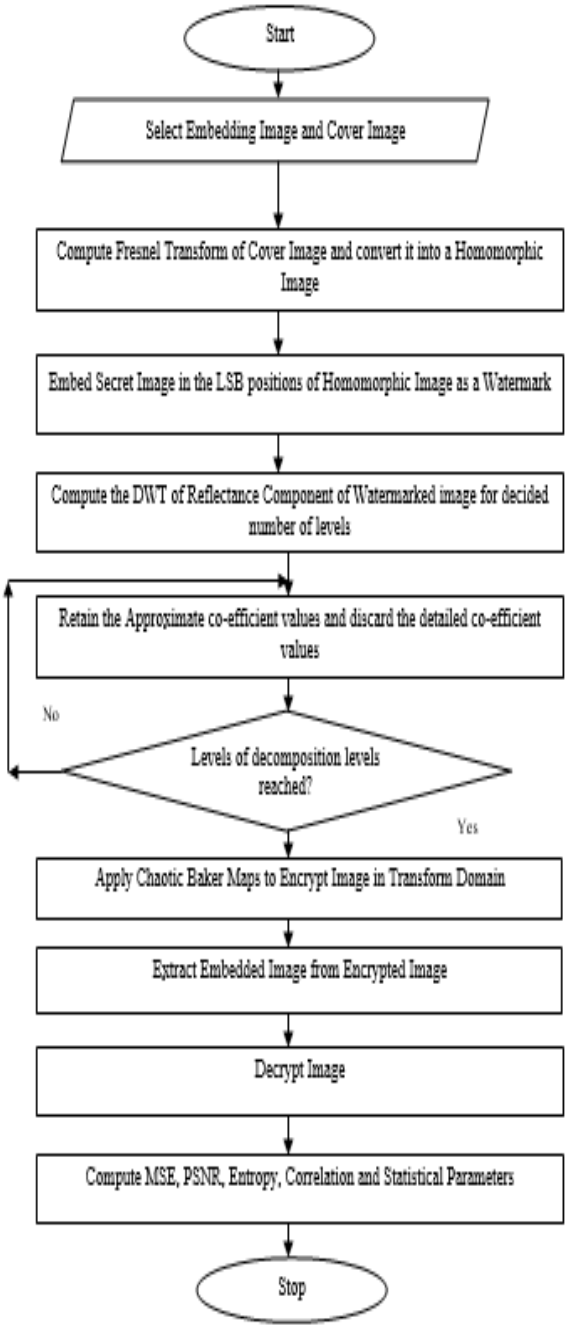

Fig.4 Flowchart of Proposed Work

IV. EXPERIMENTAL RESULTS

The system has been implemented on Matlab 2018a. The results obtained have been presented sequentially.

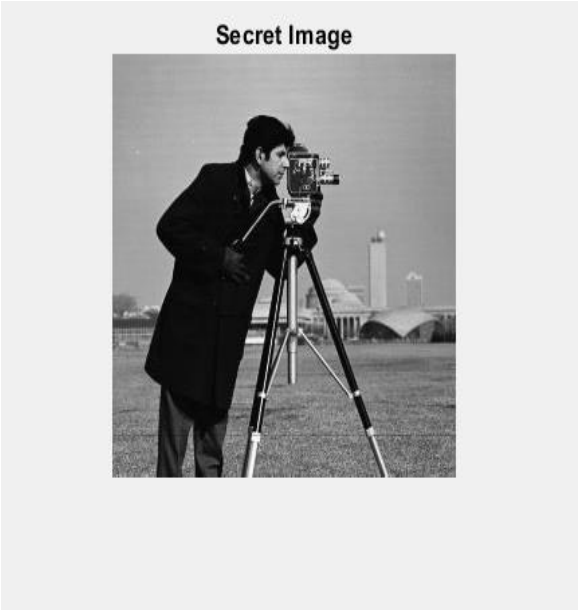

Fig.5 Secret Image

Fig. 6 Cover Image

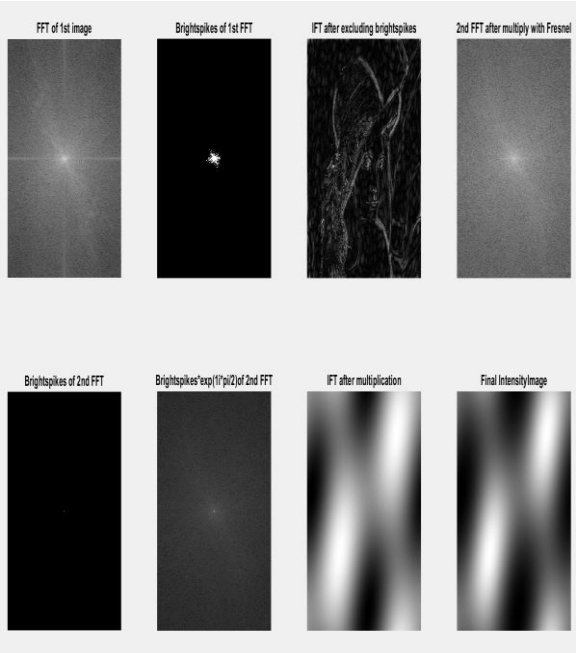

Fig. 7 Fresnel Transform Computation of Cover Image

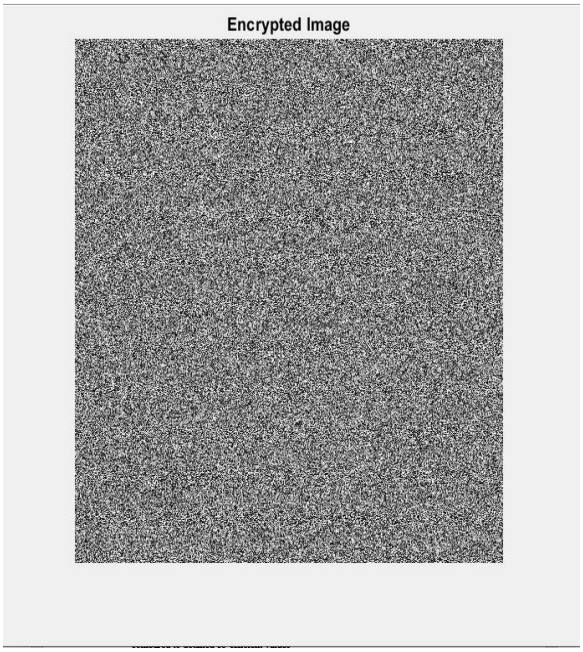

Fig. 9 Homomorphic Encrypted Image

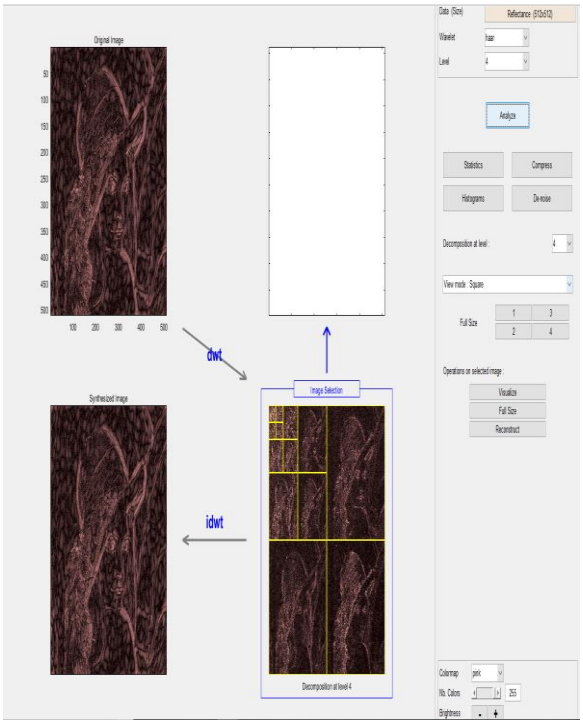

Fig. 8 4th Level DWT decomposition of the Reflectance

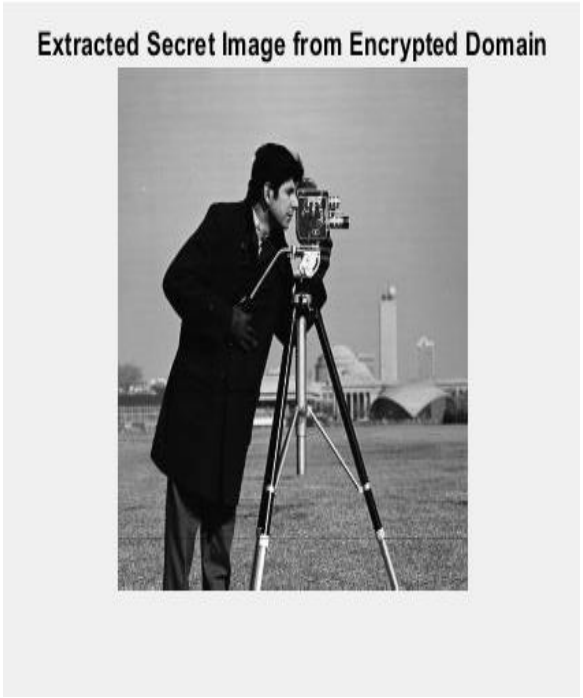

Fig. 9 Extracted Secret Embedded Image from Encrypted Domain

Table 1. Summary of Results

S.No.	Parameter	Value
1.	Image Size	512 x 512
2.	MSE	1.0838
3.	PSNR	82.8905
4.	Entropy	7.1138
5.	Correlation	0.9934
6.	Maximum Embedding Rate	1
7.	Database	USC-SIPI Image Database

The table above depicts the values of the obtained parameters for the benchmark data set image. A comparative analysis with pervious work in terms of the PSNR is tabulated in table 2.

Table 2. Comparison with Previous Work

S.No.	Approach	Avg. PSNR
1.	Reversible data hiding by Homomorphic Encryption (Wu et al.. [1])	57dB
2.	Reversible Data Hiding by Block Expansion (Jung et al., [2])	39.07dB
3.	Non blind predictive edge LSB injection method (Chokroborty et al. [3])	65.7dB
4.	Uncorrelated color space LSB Substitution (K. Mohammad et al. [4])	52.4555dB
5.	**Proposed Method**	**82.8905dB**

It can be observed from table 2, that the proposed approach employing the encryption of the reflectance component alone based on Fresnel Transform and subsequent LSB substitution based on the DWT co-efficients for separation of the critical information and details clearly outperforms the conventional LSB substitution mechnaisms.

The proposed method thus attains higher PSNR value compared to existing baseline techniques with low MSE values thereby rendering high level of security along with relatively high trustworthiness in terms of image quality (high PSNR). Thus the proposed method strikes a balance between attaining security as well as reliability for encryption systems.

Conclusion: It can be concluded from the previous discussions that using the proposed system, it possible to obtain embedded data can be extracted from the encrypted domain itself without the mandatory necessity of first decrypting the image thereby making the secret image extraction faster and less perceptible. The evaluation of the proposed technique is done based on the histogram analysis, the MSE, PSNR, Correlation and Entropy. It has been shown that the proposed system performs better compared to the previously existing technique in terms of the PSNR for the same image from the benchmark USC-SIPI image dataset.

References:

[1] H.T.Wu, Y.M.Cheung, Z.Yang, S.Tang, "A high-capacity reversible data hiding method for homomorphic encrypted images", Journal of Visual Communication and Image Representation, Vol-62, Elsevier 2021

[2] K.H. Jung, "High-capacity reversible data hiding method using block expansion in digital images", Volume-14, Springer 2020

[3] Somendu Chokroborty, Anand Singh Jalal, Charul Bhatnagar, "LSB based non blind predictive edge adaptive image steganography", Volume-76, Issue-6, Springer 2019

[4] K.Mohammad, M.Sajid, I Mehmood "Image steganography using uncorrelated color space and its application for security of visual contents in online social networks", Elsevier 2018

[5] H.Dadgostar, F.Afsari, "Image steganography based on interval-valued intuitionistic fuzzy edge detection and modified LSB", Volume-30, Elsevier 2017

[6] Xinyi Zhou, Wei Gong, WenLong Fu, Liang Jin, "An Improved Method for LSB based color image steganography combined with cryptography", IEEE 2016

[7] Bin Li, Ming Wand, Xiaolong Li, Shunquan Tan, Jiwu Huang, " A strategy of clustering modification directions in Spatial Image Steganography", Vol-10, Issue-9, IEEE Transactions 2015

[8] Bi Li, M Wang, J Huang, X Li, "A New Cost Function for Spatial Image Steganography", IEEE 2014.

[9] Mansi S, Vijay H Mankar, "Current Status and Key Issues in Image Steganography: A Survey", Volume-13, Elsevier 2014

[11] Zhenxing Qian, Xinpeng Zhang, Shuozhong Wang, "Reversible Data Hiding in Encrypted JPEG Bitstream", IEEE 2014

[12] A Bakhshandeh, Z Eslami "An authenticated image encryption scheme based on chaotic maps and memory cellular automata", Elsevier 2013.

[13] K Gu, G Zhai, X Yang, W Zhang, "A new reduced-reference image quality assessment using structural degradation model", IEEE 2013

[14] YW Tai, S Lin, "Motion-aware noise filtering for de-blurring of noisy and blurry images", IEEE 2012

[15] A. Kanso and M. Ghebleh, "A Novel Image Encryption Algorithm Based on a 3D Chaotic Map", Elsevier 2012

[16] Xinpeng Zhang, "Lossy Compression and Iterative Reconstruction for Encrypted Image", IEEE 2011

[17] W Hong, TS Chen, HY Wu, "Reversible An improved reversible data hiding in encrypted images using side match", IEEE 2011

[18] Seyed Mohammad Seyedzade, Reza Ebrahimi Atani, Sattar Mirzakuchaki, "A Novel Image Encryption Algorithm Based on Hash Function", IEEE 2010

[19] Ismail Amr Ismail, Mohammed Amin and Hossam Diab, "A Digital Image Encryption Algorithm Based A Composition of Two Chaotic Logistic Maps", International Journal of Network Security 2010

[20] CK Huang, HH Nien, "Multi chaotic systems based pixel shuffle for image encryption", Elsevier 2009

[21] R Rhouma, S Meherzi, S Belghith, "OCML-based colour image encryption", Elsevier 2009

[22] T Gao, Z Chen, "A new image encryption algorithm based on hyper-chaos", Elsevier 2008

[23] KW Wong, BSH Kwok, WS Law, "A fast image encryption scheme based on chaotic standard map", Elsevier 2008

[24] YW Zhang, YM Wang, XB Shen, "A chaos-based image encryption algorithm using alternate structure", Springer 2007

[25] L Chuanmu, H Lianxi, "A new image encryption scheme based on hyperchaotic sequences", IEEE 2007

[26] A Mitra, YVS Rao, SRM Prasanna, "A new image encryption approach using combinational permutation techniques", Citeseer 2006

[25] JF Barrera, R Henao, M Tebaldi, R Torroba, "Multiple image encryption using an aperture-modulated optical system", Elsevier 2006

[27] Y Mao, G Chen, "Chaos-based image encryption", Springer 2005

[28] D Socek, S Li, SS Magliveras, "Enhanced 1-d chaotic key-based algorithm for image encryption", IEEE 2005

[29] SS Maniccam, NG Bourbakis, "Image and video encryption using SCAN patterns", Elsevier 2004

[30] S Lian, J Sun, Z Wang, "A novel image encryption scheme based-on JPEG encoding", IEEE 2004