A SECURED HYBRID WATERMARKING TECHNIQUE USING HWT WITH LOGISTIC CHAOTIC ENCRYPTION

Antony Sudha K1, Cibi Castro V2, MuthuLakshmi G3, Ilam Parithi T4
1Research Scholar, Dept. of CSE, Manonmaniam Sundaranar University, Abishekappati, Tirunelveli, India, Email: melosudha@gmail.com
2Research Scholar, Dept. of CSE, Manonmaniam Sundaranar University, Abishekappati, Tirunelveli, India, Email: cibicastro07@gmail.com
3Assistant Professor, Dept. of CSE, Manonmaniam Sundaranar University, Abishekappati, Tirunelveli, India, Email: lakshmimsucse@gmail.com
4Assistant Professor, Dept. of CS, Manonmaniam Sundaranar University College, Puliangudi, Tenkasi, India, Email: iparithy@gmail.com

ABSTRACT:

In digital world, Internet and network applications developing faster day by day. The internet is an efficient tool for today’s communication. Security is also an important factor for data transformation over the internet. Digital watermarking is one of the effectual methods to secure the digital data from an unsecured transformation over the network. The watermark is used to express the ownership of a specific product. Encryption is also one of the solutions to the security problem. Encryption is the process of converting a readable image to unreadable image. The main characteristics of Encryption are used for identity and differentiate one encryption technique from another technique. Its ability is to secure the protected data against attacks, and its speed and efficiency. Here some encryption algorithms and watermarking techniques are compared. The better algorithms are chosen based on the performance of the metrics. In this proposed technique Hyper analytic Wavelet transform (HWT) used for watermarking and logistic chaotic is used for encryption. This proposed technique conquered the problem of security and authentication related issues.

Keywords: Hyper analytic Wavelet Transform, Logistic Chaotic, Watermarking, Encryption.

I. INTRODUCTION

In recent trends Internet, Multimedia technologies (Text, Image, and Sound) in digital form are increased. In this direction Security of data and authentication has become an essential issue. Digital watermarking is one of solutions for that problem. It is used to defend the copyright of digital images. In watermarking the secret information is embedded in the cover image. It has two categories, they are blind and non-blind. In the Non-blind method the cover image is needed in extraction process. In the Blind method the cover image is not needed in extraction process [2]. The Watermarking techniques are classified into two types based on domain, that is spatial domain and the frequency domain [3]. A pseudorandom sequence is adjoined to the cover image in some critically sampled domain and the water marked image is obtained by inverse transforming the modified image co-efficient. The Discrete Cosine Transform (DCT), The Discrete Fourier Transform (DFT) and the Discrete Wavelet Transform (DWT) are some Transformation domain [7]. Wavelet is a function that waves above and below the X-axis with varying frequencies limited duration and zero average value. The main drawback of the wavelet transform is its low ability to catch the directional information. To overcome this limitation, multi-scale and directional representations are used. Some of the multi-scale transforms are contourlet, curvelet, and shearlet [4-6], the existing techniques have various disadvantages such as attacks on the watermarked image, Sensitive to filters and hostile attacks can destroy the watermark image [7]. The other wavelet transforms such as the Double Tree Complex Wavelet Transform (DTCWT) [8], the Hyper analytic Wavelet Transform (HWT) [9] could also be considered. DTCWT and HWT are compared to DWT, quasi-shift invariance and enhanced directional selectivity is the advantages, and also data hiding capacity and redundancy also increases. Encryption is a method for a user to securely share data or image over an insecure network. Security is an essential part of communication through network. There are many algorithms that are available for encrypting the data or image. Encryption is the process in which the plain text has
been completed into the cipher text, which means readable form into an unreadable form. There are two types of private key encryption algorithms that is stream cipher and block ciphers. Block Cipher is one type of private key encryption algorithm, block means a fixed length group of bits. It converts the plaintext into cipher text by taking plaintext’s block at a time. Stream Cipher is another type of private key encryption algorithm. It converts the plaintext into cipher text by taking bits or byte one by one at a time. A dynamic system is called chaotic. Where a very small variation in its initial state produces macroscopic differences in the final result. Chaos theory is a study of dynamical systems. Chaotic encryption means the messages are encrypted using pseudorandom sequences generated by chaotic systems. Qian Gong-bin, Jiang Qing-feng, Qiu Shui-sheng [14], proposed an image encryption method based on Data Encryption Standard algorithm and chaotic encryption. The chaotic sequence is implemented in the DES algorithm to improve the initial keys and the iterating operations, so that the chaotic encryption is combined with DES algorithm. In this algorithm make full use of chaotic system’s sensitivity to initial value is assigned. Manjula K G, M N Ravikumar [11], proposed “Color Image Encryption and Decryption using DES Algorithm”. DES algorithm is utilized to image file encryption and decryption. DES guarantees the unbreakable security for color image. The implementation approach shows the encrypted and decrypted image and also historical analysis is done with enhanced techniques. P. Karthigaikumar, Soumiya Rasheed [13], proposed the design of a 128 bit encoder using AES Rijndael Algorithm for image encryption. The encryption process is iterative in nature. Each iteration is known as rounds. For each round 128 bit input data and 128 bit key is required. That is, in needed of words key in one round. So the input key must be expanded to the required number of words, which depends upon the number of rounds. The output of each round serves as input of next stage. In AES system, same secret key is used for both encryption and decryption. So it provides simplicity in design. A chaos-based color image cipher with an efficient substitution key stream generation strategy. The hyper chaotic Lu system and logistic map are employed to generate the permutation and substitution key stream sequences for image data scrambling and mixing. In the permutation stage, the positions of colored sub pixels in the input image are scrambled using a pixel swapping mechanism. In the substitution stage, an efficient key stream generation method that can be extracted the three key element sequences from the current state of the iterative logistic map [12]. Hazem Mohammad Al-Najjar and Asem Mohammad Al-Najjar [15], proposed an image encryption based on logistic map chaotic function is discussed. The encryption system can be divided into two approaches as pixel replacement approach and pixel scrambling approach. In pixel replacement approach, the pixel values are changed where as in pixel scrambling the pixel positions are changed. This algorithm consists of 2 replacement approaches to change the value of the pixel without shuffling the image itself. To achieve this, two pixel mapping tables that are created by using the logistic map are used. The pixel mapping table (PMT) contains the pixel values from 0 to 255 in the shuffled order with the size 256x1. The algorithm uses only replacement approaches to encrypt the image. The two different replacement approaches are: in the first approach, the pixels are shifted by using a random value and mapping it by using PMT. In the second approach, replacement is done by using the XOR operation with specific random vector generated by using the logistic map. The process of decryption is done in the reverse order.

II. COMPARED ENCRYPTION ALGORITHMS

Encryption makes the modern world go round. Every time make a mobile phone call, buy something with a credit card in a shop or on the web, or even get cash from an ATM, encryption grant upon that transaction the confidentiality and security to make it possible. Encryption is based on the ancient art of cryptography that uses computers and algorithms to turn plain text into an unreadable, jumbled code. To decrypt that cipher text into plaintext, need an encryption key, a series of bits that decode the text. The key is something only the intended recipient has in their possession. In this section the three encryption algorithms such as DES, AES, and chaos based algorithm are compared based on their performance.

2.1 Data Encryption Standard (DES)

Most of the block cipher techniques will be followed common structure, which is feistel structure. Plain image divided into two equal halves and performs the round function and apply the individual keys to each and every round and then swap the two halves, this the process of feistel structure. DES is a one of the block cipher algorithm. It follows the feistel structure. In DES the plaintext processes to cipher text in a number of blocks. Here the block size of plain text is 64 bit; the number of rounds in DES is 16 bit. If any block cipher follows the feistel structure that means the plaintext is processes the number of rounds, each round should have the sub keys. In DES number of round is 16, so it generates 16 sub keys. Sub key size is 48 bit. From the 64 bit key have to generate sixteen 48 bit sub keys. Each and every round has to use each sub keys. Finally the cipher text is converted into 64 bit cipher text. This is an over view of Data Encryption Standard (DES).
2.1.1 Left Circular Shift
Left Circular Shift means number of bits to be shifted depends upon the round.

<table>
<thead>
<tr>
<th>Rounds</th>
<th>Shift</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 2, 9, 16</td>
<td>One bit</td>
</tr>
<tr>
<td>Others</td>
<td>Two bit</td>
</tr>
</tbody>
</table>

2.1.2 Substitution Box (S-Box)
DES algorithm has 8 S-box. Here the input is 48 bit and output is 32 bit. 48 bit divided in 8 S-Box. Each S-Box has 6 bit as input, two bits are reduced and give four bits as output. Totally the output produced is of 32 bits.
2.1.3 Round function of DES

In DES 64 bit plain text is divided into two 32 bit half, that is left 32 bit and right 32 bit. Key is also divided into two half, left 28 bit key and right 28 bit key. 32 bit right half is given an input to the Expansion Permutation. In this function additional 16 bits are added in the 32 bit, so as to get 48 bit and this must be XOR with Key. In key left and right 28 bit keys apply to the Left Circular Shift (LCS). After the LCS apply the permuted choice 2. Permuted choice 2 produce 48 bit key is output. After XOR operation get 48 bit. This is given an input to S-Box. In S-Box operation 48 bit reduces to 32 bit. After the S-box function apply the permutation function, then get 32 bits and this is XOR with left 32 bit , this output store in right half and then right 32 bit half store in left half. These are the inputs for next round. After applying the left circular shift store it in left and right key . These are inputs for next key generation.

2.1.4 Expansion Permutation

Expansion permutation means expanding the number of bits that is 16 bits to be added, and re-arranging the order of bit position according to given transposition order. The complete length of the expansion permutation becomes 48 bit.

2.1.5 Permuted Choice 1

In permuted Choice 1 will eliminate the multiple of 8. Thus the output comprises of 56 bit.
2.2 Advanced Encryption Standard (AES)

AES encryption is a method of scrambling data. A key is used to mix up data such that it can be securely stored or transferred over the network, and only persons with the key can unscramble the data. It is a symmetric key encryption algorithm. This means the same key is used to scramble the data and unscramble it. In AES the message is having the plain text and secret key, and combined it comes as an input in 128 bits, and it will go for the cipher block that is 128 bit (Secret key and plaintext). It can also 192 bit and also 256. No other bit supports in AES design, so based on the information 128, 192, 256 will go the cipher engine and it will produce the cipher text. The 128 bit data block is divided into 16 bytes. These bytes are mapped to a 4x4 array called the State, and all the internal operations of the AES algorithm are performed on the State.

![Flow diagram for AES](Fig 2.3. Flow diagram for AES)

2.3 Chaotic Logistic Map

The logistic map is a second degree polynomial widely used in different arrays, expressed by the following recurrence relation:

\[ X_t = \lambda X_t (1 - X_t) \]  

(1)

Where \( \lambda = 3.57, 4 \) is a control parameter of the logistic map, the variable \( X_t \) is a control parameter of the logistic map, the variable \( X_t \) is the iterations number used to generate the iterative values. When varying the parameter of the logistic map \( \lambda \), we see that for a good choice of the initial condition \( X_0 \), the chaotic nature occurs only when \( \lambda = 3.57, 4 \). The following algorithm is used for logistic chaotic encryption.
Algorithm for logistic Chaotic Encryption

\[
\begin{align*}
P & \leftarrow \text{Plain Image} \\
[r \ s] & \leftarrow \text{Size of (P)} \\
N & \leftarrow r \times s \\
m(1) & \leftarrow \text{initial value} \\
\text{for } i : 1 \text{ to } N-1 \\
\text{begin} \\
m(i+1) & \leftarrow R \times m(i) - m(i)^2; \\
\text{end} \\
m & \leftarrow \text{mod}(1000 \times m, 256); \\
n & \leftarrow 1; \\
\text{for } i : 1 \text{ to } a \\
\text{begin} \\
\text{for } j : 1 \text{ to } b \\
\text{begin} \\
\text{encrypted _image(i,j) } & \leftarrow \text{XOR}(m(n), P(i,j)); \\
n & \leftarrow n+1 \\
\text{end} \\
\text{end} \\
\text{write encrypted_image} \\
\text{end}
\end{align*}
\]

III. COMPARED WATERMARKING TECHNIQUES BASED ON FREQUENCY DOMAIN

3.1 Discrete Cosine Transform (DCT)

Discrete Cosine Transform is one of the transform in frequency domain. In frequency domain analyze signal with respect of frequency. Watermarking Techniques based on the Discrete Cosine Transformation [1]. Here, the original image divided into 8x8 blocks and then blocks reduced by dynamic range value by subtracting value 127 from each pixel value. So pixel value range lies between [-127, 127]. In this spatial value transformed into Discrete Cosine co-efficients using Discrete Cosine Transformation. DCT transformation applied to the whole image, then the image divided into different frequency band as shown in Fig 3.1.

![Fig 3.1. Different Frequency Band](image-url)
In Fig 3.1. Shows the Low Frequency band (FL), Middle Frequency band (FM), High Frequency band (FH), these are the different frequency bands in DC co-efficient. In this technique watermark is embedded in the middle frequency. Low frequency band contains the visual part of the image and high frequency band removed by the quantization process. In the middle frequency visibility of image remains unstirred.

In Fig 3.2. Shows the embedding process of DCT. Here the input image is split into 8x8 blocks and then reduced by dynamic range. The reduced values given to input of DCT. After discrete Cosine Transformation DC co-efficient are produced. These co-efficients given to the input of quantization process. The watermark image also has same process as far as quantization. In watermark image multiply with Strength factor $\alpha$, and then add to cover Quantized image. This output is given to an input of Inverse Quantization and then applying Inverse DCT then Inverse Reduced dynamic range. Finally get the watermarked image.

### 3.2 Discrete Wavelet Transform (DWT)

Discrete wavelet transform is frequency domain analysis method. It is based on wavelets and it performs wavelet decomposition using wavelet filters such as Daubechies, Haar, Coiflets. The advantage of DWT is wavelets are certained in time and frequency around a particular point. In this frequency domain watermarking technique proved to be more effective with respect to achieving the imperceptibility and robustness requirements of digital watermarking algorithm. In DWT an image is decomposed into four sub-bands LL, LH, HL, HH by first level as shown in Fig 3.3.

![First level DWT decomposition of an image](image-url)
In Fig. 3.3 shows DWT after the first level decomposition, the DWT applied to LL band which decompose this band into four sub bands, LL1, LH1, HL1, HH1.

In Fig. 3.4 shows embedding process the input image and watermark image is given an input to 2D DWT. DWT coefficients for input image added to DWT coefficients for watermark image multiply with strength factor $\alpha$ (0.1). After that Inverse 2DWT to be applied then obtain the watermarked image.

### 3.3 Hyperanalytic wavelet transform (HWT)

Hyperanalytic wavelet transform is an extension of analytic wavelet decompositions. It is quasi shift-invariant and it has a good directional selectivity. In this transform no need the construction of any special wavelet filter. An ideal Hilbert transformer was considered.
HWT implementation shown in the Fig 3.5. Hyperanalytic wavelet transform of the image can be computed with the help of 2D-DWT. Discrete wavelet transform applied to hyper complex image. HWT has four trees. In first tree the 2D DWT is applied to the input image. In the second tree 2D DWT is applied to the one dimensional Hilbert transforms computed across the rows(Hx).The Third tree 2D DWT is applied to the one dimensional HT computed across the columns (Hy). The fourth tree is 2D DWT is applied to the result obtained after computation of the two ID HT of the image. Hyper analytic wavelet transformed image obtained with the help of reverse process of construction of HWT. In embedding process the input image and watermark image are given an input to 2D HWT. HWT co-efficients for input image added to HWT co-efficients for watermark image multiply with strength factor α (1.5).After that Inverse 2D HWT to be applied then obtain the water marked image. In Fig.9 shows embedding process the input image and watermark image.
IV. PROPOSED WATERMARKING TECHNIQUE

In this proposed system, Hyper analytic Wavelet Transform (HWT) is used for watermarking, and logistic chaotic algorithm is used for watermark Encryption Process. The following diagram shows the block diagram of proposed watermarking Technique.

In this proposed watermarking technique, the input image given to the input of 2D Hyper Analytic Wavelet Transform (HWT). Hyper Analytic Wavelet Transform is used to convert the input image into hyper complex image. Watermark image should be encrypted using logistic chaotic encryption. In this encryption process the logistic mapping function applied to the watermark image. It produced key matrix. In logistic mapping initial parameters are very sensitive to produce key matrix. Small changes in these initial parameters have some big variant in the output. The Key matrix is XORed with original image and gets the encrypted watermarked image. Encrypted watermark image given an input of the 2D HWT. After complete the Hyper-analytic wavelet transform as embed with original complex image, and then Inverse 2 DWT process applied to the embedded image. Finally get the watermarked image.
V. RESULTS AND ANALYSIS

This section represents analysis of proposed watermarking Technique. It is programmed in Matlab. The proposed technique is implemented and tested on three natural original images are size of 256 X 256. The constructively embedded the natural watermark image of size 32 X 32 into the original image. The encryption algorithms are tested on two parameters encryption time and PSNR values. The encryption time means the time that an encryption algorithm takes to generate a cipher text from a plain text. Experimental result reveals that the chaotic logistic map algorithm produced a better result with very low encryption time when compared with the other two methods.

![Sample test original Images](image_url)

Fig 5.1. Sample test original Images

![Encrypted and Decrypted Images](image_url)

Fig 5.2. (a) Original watermark image, (b) DES encrypted images, (c) AES encrypted images, (d) Chaotic encrypted images, (e) Decrypted images

Table.1 shows the Comparative analysis of DES, AES and Logistic Map algorithm based on PSNR values.

<table>
<thead>
<tr>
<th>Images</th>
<th>DES</th>
<th>AES</th>
<th>Logistic Map</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strawberry</td>
<td>32.56</td>
<td>36.91</td>
<td>39.91</td>
</tr>
<tr>
<td>Butterfly</td>
<td>35.29</td>
<td>46.98</td>
<td>53.12</td>
</tr>
<tr>
<td>Sun Flower</td>
<td>32.81</td>
<td>39.21</td>
<td>45.31</td>
</tr>
<tr>
<td>Airplane</td>
<td>39.28</td>
<td>49.28</td>
<td>56.42</td>
</tr>
<tr>
<td>Onion</td>
<td>36.12</td>
<td>44.58</td>
<td>52.26</td>
</tr>
</tbody>
</table>
Table 2. Comparative analysis of encryption algorithms based on Encryption Time

<table>
<thead>
<tr>
<th>Images</th>
<th>DES(s)</th>
<th>AES (s)</th>
<th>Logistic Map (s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strawberry</td>
<td>0.8560</td>
<td>0.6234</td>
<td>0.4876</td>
</tr>
<tr>
<td>Butterfly</td>
<td>1.0326</td>
<td>0.9365</td>
<td>0.6572</td>
</tr>
<tr>
<td>Sun Flower</td>
<td>0.6678</td>
<td>0.5230</td>
<td>0.4267</td>
</tr>
<tr>
<td>Airplane</td>
<td>1.5672</td>
<td>1.0538</td>
<td>0.7560</td>
</tr>
<tr>
<td>Onion</td>
<td>0.9452</td>
<td>0.5381</td>
<td>0.3546</td>
</tr>
</tbody>
</table>

5.1 Histogram Analysis
A well encrypted image should have a histogram with a uniform distribution. Compared algorithms were tested.

![Histogram Analysis](image)

Fig 5.3. a) Original image b) Encrypted image using DES c) Encrypted image using AES, d) Encrypted image using Logistic map e) Histogram for original image f) Histogram for DES encrypted image g) Histogram for AES encrypted image h) Histogram for logistic map encrypted image

The watermarked images possess superior Peak Signal to Noise Ratio (PSNR) and Normalized Correlation.

Table 3. Comparative analysis of watermarking techniques based on PSNR values

<table>
<thead>
<tr>
<th>Images</th>
<th>DCT</th>
<th>DWT</th>
<th>HWT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Airplane</td>
<td>27.05</td>
<td>49.21</td>
<td>58.52</td>
</tr>
<tr>
<td>Lotus</td>
<td>29.71</td>
<td>52.13</td>
<td>61.37</td>
</tr>
<tr>
<td>Flower</td>
<td>23.45</td>
<td>45.05</td>
<td>53.52</td>
</tr>
</tbody>
</table>
Table 4. Comparative analysis of watermarking techniques based on NC values

<table>
<thead>
<tr>
<th>Images</th>
<th>DCT</th>
<th>DWT</th>
<th>HWT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Airplane</td>
<td>0.69</td>
<td>0.72</td>
<td>0.91</td>
</tr>
<tr>
<td>Lotus</td>
<td>0.75</td>
<td>0.84</td>
<td>0.97</td>
</tr>
<tr>
<td>Flower</td>
<td>0.61</td>
<td>0.81</td>
<td>0.92</td>
</tr>
</tbody>
</table>

Different attacks are performed on the watermarked images to facilitate the robustness of the compared techniques. Fig 9. shows the different attack cover images such as Intensity adjustment, Noise, Blurring, Unsharp filter.

![Airplane](image1)

(a) Airplane

![Intensity adjustment](image2)

(b) Intensity adjustment

![Blurring](image3)

(b) Blurring

![Unsharp Filter](image4)

(c) Unsharp Filter

![Noise](image5)

d) Noise.

Fig 5.6. Attacked Cover images

The attack is applied on the watermarked image and after that cover and watermark images are extracted it.

VI. CONCLUSION

Frequency domain techniques act in a main role of digital watermarking. This paper, proposed a new watermarking technique based on Hyper Analytic Wavelet Transform with Logistic map Encryption. Chaotic based algorithm shows better results due to their excellent characteristics, which is revealed from table 1 and table 2. Results and analysis shows that the chaotic based logistic map encryption algorithm is an effective method for image encryption. Histogram analysis demonstrates logistic map that has the high sensitive dependence of the encryption and decryption. The Hyper Analytic Wavelet Transform based watermarking technique has a better ability than the DCT and DWT based Techniques. HWT is adequate technique for embedding process and it has a flexible structure also. The performance of the HWT algorithm can be improved by using Soft Computing Techniques.
REFERENCES


