ISSN 2348 – 7968

Nesting of Image Watermarking Using RLSB Technique

V. Aruna, R. Selvakumar M.E

M.E Communication Systems, Infant Jesus College Of Engineering And Technology

Abstract:

The main objective of this paper is image watermarking. This paper a new technique is proposed to improve the LSB scheme i.e. Randomized LSB (RLSB). Randomized LSB (RLSB) hiding technique used, because it is having the lesser complexity and also its approach is more robust (strong) towards the variations in the type of image. This algorithm is used here for embedding one image with another and the blowfish algorithm is used here to encrypt the watermark image before performing the embedding process with the cover image (main image).The blowfish algorithm is a symmetric key block cipher technique which will be effectively used for the process of encryption and also for the safeguarding of the data. It basically takes a key of variable-length (from 32 bits to 448 bits), which makes it an ideal algorithm for securing the data. Here the encryption of watermark image takes place before it gets embedded with the main image (means cover image) so as to get the higher security of the watermark image. The research is primarily focus on to getting the higher secured watermark. Thus we do not use to encrypt or decrypt the whole image, but we use to perform these operations only on some selected pixels. And the result is evaluated on the basis of PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error) calculation.

1. Introduction:

A digital watermark is a kind of marker covertly embedded in a noise-tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal; the hidden information should, but does not need to contain a relation to the carrier signal. Digital watermarks may be used to verify the authenticity or integrity of the carrier signal or to show the identity of its owners. It is prominently used for tracing copyright infringements and for banknote authentication. Digital watermarking is the act of hiding a message related to a digital signal (i.e. an image, song, video) within the signal itself. It is a concept closely related to steganography, in that they both hide a message inside a digital signal. However, what separates them is their goal. Watermarking tries to hide a message related to the actual content of the digital signal, while in steganography the digital signal has no relation to the message, and it is merely used as a cover to hide its existence. One of the first applications for watermarking was broadcast monitoring. It is often crucially important that we are able to track when a specific video is being broadcast by a TV station. This is important to advertising agencies that want to ensure that their commercials are getting the air time they paid for. Watermarking can be used for this purpose. Information used to identify individual videos could be embedded in the videos themselves using watermarking, making broadcast monitoring easier.

2. Related Work:

P Gupta [2] had used the concept of Cryptography based Digital image watermarking technique to enhancing the security of the watermark data with the use of blind watermarking technique where it uses Watermark nesting and encryption and for the encryption process, the XOR operation was used and technique based on DWT used for embedding the watermarked watermark image in cover image (main image). J S Bhalla and P Nagrath [3] introduced Nested Digital Image Watermarking technique using the blowfish algorithm. In this work, they mainly focus on increasing the embedding capacity of the watermarks and also improving the security of watermark by using the concept of LSB hiding for embedding process. Here one watermark gets encrypted by using the blowfish algorithm and then gets embedded into another watermark image (using the LSB method). Then this nested watermark image is again encrypted and finally gets embedded with the main image. Authors D Biswas, D Sarkar, A Pal [4] proposed that the direct LSB hiding technique has the drawback of having greater complexity and its dependency on the type of images whereas Randomized LSB that means RLSB technique scores more in terms that it has the lesser complexity (and also more robust to variations in the type of image) by considering the PSNR values (Peak Signal to Noise Ratio). The research work proposed by authors S P Singh, R Maini [5] shows the performance comparison between the most of the common encryption algorithms that is (DES, 3DES, Blowfish, AES) and they conclude that the Blowfish algorithm has better performance as compared with the other encryption algorithms (mentioned above) and also that it has no known security weak points (so far). Here the authors did the comparison on the basis of (processing different sizes of data blocks by algorithm) to determine their encryption decryption speed. The concept of LSB Based Lossless Digital Image Watermarking (using Polynomials in Spatial Domain) for DRM was introduced by A. Siva Sankar, T. Jayachandra Prasad, M.N. Giri Prasad [6] in which they introduced a new concept of embedding method in which it randomly hides the messages in the form of LSB of any component (of the chosen pixel) using polynomial and thereby the probability of getting the right coefficient correctly is quite difficult.

There are many limitations in the existing system. This paper proposes the watermarking using the RLSB technique. Chapter 3 discuss about the methods in the proposed system. Chapter 4 shows the results and conclusion of this paper.

3. Methodology:

The overall block diagram shows below. The diagram shows the whole methods in the watermarking system.

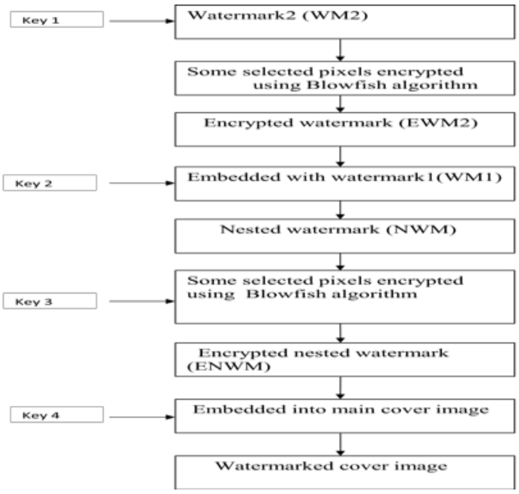

Key 1
Watermark2 (WM2)
Some selected pixels encrypted using Blowfish algorithm
Encrypted watermark (EWM2)
Key 2
Embedded with watermark1(WM1)
Nested watermark (NWM)
Key 3
Some selected pixels encrypted using Blowfish algorithm
Encrypted nested watermark (ENWM)
Key 4
Embedded into main cover image
Watermarked cover image

Fig: 1Overall Diagram

3.1 Blowfish Encryption Algorithm:

Blowfish Algorithm is a Feistel Network, iterating a simple encryption function 16 times. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. It is significantly faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches. Below figures show brief about working of blowfish algorithm.

Embedding the digital watermark

Step 1. Two images are taken as input:
First of all, the cover image is taken as input. Then the message or information logo is taken as input. The cover image is taken to be a gray scale image. The logo or information is a binary image basically a sequence of 0's anda 1's.
Step 2. The size of the images is extracted:
Next to make the program compatible to run for any size of the cover image and information logo keeping in mind the data carrying capacity of the cover image the dimensions of the respective images are extracted and stored in to two variables..
Step 3. Normalize and reshape the logo:
After normalizing the information logo it is being reshaped in one dimension.
Step 4. Transforming the cover image into wavelet domain using DWT:
The cover image is transformed to wavelet domain using discrete wavelet transform. Here we use 'haar' transform to do the DWT. Here the 1st level DWT was used to obtain more capacity for hiding the information. The cover image is decomposed into 4 sub domains as
HH, HL, LH and LL according to different frequencies of the cover image.
Step 5. Calculate the length of transformed cover image and 1 D logo
Step 6. Calculate the size of each sub domain decomposed cover image and reshape them in to 1D
Step 7. Determine the maximum coefficient value of each of the 4 sub domain
Step 8. Finding the position to hide the information logo into the transformed logo: The position for hiding the binary logo in each sub domain must be in between zero and the maximum coefficient value of that sub domain.
Step 9. Hiding a number of sets of same information logo in HL and LH domain: More than one set of same information is being hidden in HL and LH band or domain for easier and good quality recovery. The hiding process in each of these domains follows a specific formula. The formula is that the black dots in each sets of 1D information logo is hidden in a position of information logo position from where a constant value is subtracted.
Step 10. Reshaping the decomposed image back to its normal dimension
Step 11. Write the watermarked image to a file and display it.

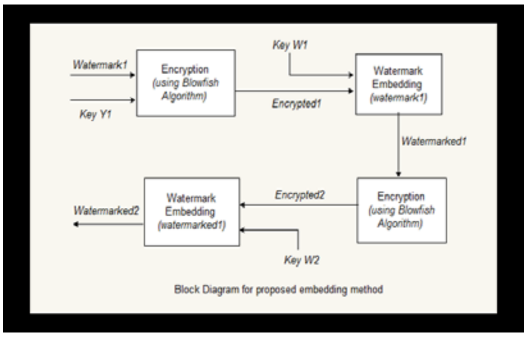

Watermark1
Key Y1
Encryption (using Blowfish Algorithm)
Key W1
Encrypted1
Watermark Embedding (watermark1)
Watermarked1
Encryption (using Blowfish Algorithm)
Encrypted2
Watermark Embedding (watermarked1)
Key W2
Watermarked2
Block Diagram for proposed embedding method

Fig 2 Block Diagram of Embedded method

Recovery of the embedded watermark

We have assumed that the cover image that is hiding the watermark is available at the receiving end. So again in the process of recovery we first take the original image that has been used to hide the information. Along with that we also send the receiver of the message, 3 keys which essentially act as private keys. These keys are required to decrypt and to the extract the encrypted, embedded messages.
Step 1. Take input the watermarked and original image
Step 2 Find 1st level decomposition of both the two inputs using DWT
Step 3. Find the size of each sub domain of both the two decomposed input image

Step 4. Reshape each of the decomposition of both watermarked and original cover image into 1 D
Step 5. Take two input keys equal to the dimension of logo to find the size of 4 decompositions of logo
Step 6. Determining maximum coefficient values of original cover image
Step 7. Finding positions that were used to hide logo for each decomposition
Step 8. Extracting positional sets for different sets of logo from each decomposition
Step 9. Recovery of different sets of logo from each of the sub bands using majority algorithm and construction of final logo from the different recovered sets
Step 10. After reshaping display each of the recovered sets of logo and the final constructed logo

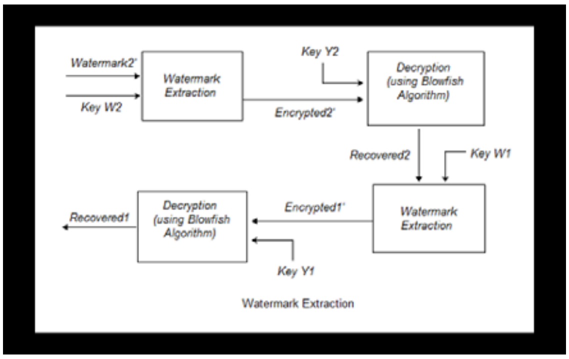


Fig 3 Block Diagram of Watermarking Extraction

3.2 Least Significant Bit Technique:

Least significant bit (LSB) insertion is a common and simple approach to embed information in an image file. In this method the LSB of a byte is replaced with an M"s bit. This technique works good for image steganography. To the human eye the stego image will look identical to the carrier image.. For hiding information inside the images, the LSB (Least Significant Byte) method is usually used. To a computer an image file is simply a file that shows different colors and intensities of light on different areas of an image. The best type of image file to hide information inside is a 24 Bit BMP (Bitmap) image. When an image is of high quality and resolution it is a easier to hide information inside image. Although 24 Bit images are best for hiding information due to their size. Some people may choose 8 Bit BMP"s or possibly another image format such as GIF . The reason being is that posting of large images on the internet may arouse suspicion. The least significant bit i.e. the eighth bit is used to change to a bit of the secret message.

Least Significant Bit Algorithm

1. Select a cover image of size M*N as an input.
2. The message to be hidden is embedded in RGB component only of an image.
3. Use a pixel selection filter to obtain the best areas to hide information in the cover image to obtain a better rate. The filter is applied to Least Significant Bit (LSB) of every pixel to hide information, leaving most significant bits (MSB).
4. After that Message is hidden using Bit Replacement method.

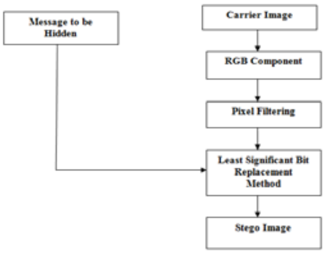


Fig: 4 LSB

3.3 Random LSB Watermarking

The main idea of LSB watermark embedding is that precision in many image formats is greater than that perceivable by average human vision Therefore; an altered image with slight variations in its colors will be indistinguishable from the original by a human being, just by looking at it. By using the least significant bits of the pixels' color data to store the hidden message, the image itself is seemed unaltered. A Random LSB embedding algorithm will be used, in which the secret data are spread out among the image data in a seemingly random manner. This can be achieved if both the sender and receiver having the same secret key or share a secure key. This key can be used to generate pseudorandom numbers, which will help extracting the secret image by defining the place and the order in which the secret data is laid out. The advantage of that method is that it incorporates some cryptography concepts that diffuse the secured data. However, it goes beyond just making it difficult for an attacker knows that there is a secret message. It also makes it harder to determine that there was a secret message in the first place. The reason is because the randomness makes the embedded message seem more like noise statistically than in the straight forward embedding method.

4. Experimental Results:

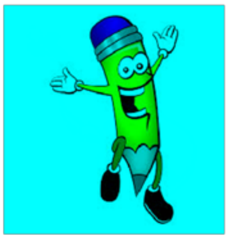
The below images are shows the results for the proposed system. The below figures are represent the different stage of watermark encryption and embedding in original and cover image

Original Image

Cover Image1

The below figures are represent the different stage of watermark encryption and embedding in original and cover image

Cover image + Original image



Cover Image2

The below figures are represent the different stage of watermark embedding and extraction in cover and original image

Watermarked Image

Recovered Image

The work has been implemented and realized using MATLAB. The result has been observed on the basis of PSNR that is (Peak Signal to Noise Ratio) calculation and MSE that is (Mean Square Error) calculation. These both are the error metrics used to compare the image compression quality. Lower the value of MSE, higher will be the quality of image. And the value of PSNR should be high. The work has been done by taking the cover image of size 800 x 800 pixels, watermark1 of size 200 x 200 pixels and watermark2 of size 48 x 52 pixels. It has been observed from the calculations that the values of MSE and PSNR get changes according to the variations in the types of attacks which were applied on the Original Image (Cover Image), Watermark Image1 (Watermark1) and Watermark Image2 (Watermark2) respectively. The result shows that the value of MSE almost tends to zero and the value of PSNR is higher. Thus we can say that the quality of image we get will be higher. [12] The PSNR value will give the measurement of distortion of the carrier image after hiding the information. In this case the signal is original data, and noise is the error which is introduced by the compression. Thus, higher the PSNR value the better will be the quality of the compressed (or reconstructed image). And when the two images will be identical, then the MSE value will become zero and for this the value of PSNR should be undefined that is ∞.

Peak Signal-to-Noise Ratio (PSNR)

The peak signal-to-noise ratio (PSNR) is used to evaluate the quality between the enhanced image and the original image. The PSNR formula is defined as follows:

$$PSNR = 10\;X\;log_{10}\frac{255\;X\;255}{\frac{1}{HXW}\sum_{x=0}^{H-1}\sum_{y=0}^{W-1}[f(x,y)-g(x,y)]^2}\;dB$$

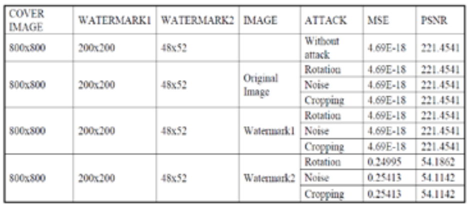
Where H and W are the height and width of the image, respectively; and f(x,y) and g(x,y) are the grey levels located at coordinate (x,y) of the original image and enhanced image, respectively.

Mean Squared Error Rate (MSE)

The mean square error or MSE of an estimator is one of many ways to quantify the difference between an estimator and the true value of the quantity being estimated. As a loss function, MSE is called squared error loss.

$$MSE = \frac{1}{n}\sum_{i=1}^{n}(\widehat{Y_\iota} - Y_i)^2$$

Where $\widehat{Y_\iota}$ is the vector of n predictions and Y_i is the vector of true values.



COVER IMAGE	WATERMARK1	WATERMARK2	IMAGE	ATTACK	MSE	PSNR
800x800	200x200	48x52		Without attack	4.69E-18	221.4541
800x800	200x200	48x52	Original Image	Rotation	4.69E-18	221.4541
				Noise	4.69E-18	221.4541
				Cropping	4.69E-18	221.4541
800x800	200x200	48x52	Watermark1	Rotation	4.69E-18	221.4541
				Noise	4.69E-18	221.4541
				Cropping	4.69E-18	221.4541
800x800	200x200	48x52	Watermark2	Rotation	0.24995	54.1862
				Noise	0.25413	54.1142
				Cropping	0.25413	54.1142

Table 5.1 Calculation of MSE & PSNR depending upon the types of attack on Original, Watermark1 and Watermark2 Image respectively

From the above figure it was observed that the value of MSE and PSNR for Original Image and Watermark1 Image when undergo through the various attacks will gives the better result as their MSE values are very low (approximately tends to zero) and PSNR values are high, which shows that quality of the image remains better after reconstruction. But we also observed that when the Watermark2 will undergo through various attacks it will not gives the better result as we saw earlier for the watermark1 and original cover image. This is because watermark2 was undergone through 2 embedding processes and 2 encryption processes. Thus its pixel gets distorted more as compare to the original and watermark1 image.

5. CONCLUSION & FURTHER DISCUSSION

The work has been carried out for the different sizes of cover images and watermark images that is watermark1 image and watermark2 image. Each image has different values for MSE and PSNR. After going through different types of attacks like Rotation, Noise and Cropping, the retrieved image will not get degraded with its originality. The quality of image has been quietly unaffected. In the proposed methodology, the main concern is to get the secured image without destroying in the quality of the original image. The main advantage of the proposed technique is that it uses the concept of nested digital image watermarking and RLSB hiding technique for embedding and extraction and blowfish algorithm for encryption and decryption, not in the whole image; but only in some selected pixels. Thus it provides more security as it is difficult to determine the values of random selected pixels. As encryption and decryption is performed using blowfish algorithm to provide more security, before embedding and extraction process respectively thus encryption and decryption process takes more time to processed the data as also it has to be applied on some selected pixels. So in future, some other algorithm should be used for encryption and decryption process.

REFERENCES

[1]. Cox, I., Miller, M., Bloom, J. Digital Watermarking, Morgan Kaufmann, Ch 1, p. 6, Web ISBN-13: 978-0-08-050459-9.

[2]. Preeti Gupta, “Cryptography based digital image watermarking algorithm to increase security of watermark data”, International Journal of Scientific & Engineering Research, Volume 3, Issue 9, September 2012 ISSN 2229-5518.

[3]. Jasdeep Singh Bhalla, Preeti Nagrath, “Nested Digital Image Watermarking Technique Using Blowfish Encryption Algorithm”, International Journal of Scientific and Research Publications, Volume 3, Issue 4, April 2013 ISSN 2250-3153.

[4]. D. Biswas, S. Biswas, P.P. Sarkar, D. Sarkar, S. Banerjee, A. Pal, “Comparison And Analysis Of Watermarking Algorithms In Color Images – Image Security Paradigm”, International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No 3, June 2011.

[5]. Simar Preet Singh, and Raman Maini, “Comparison Of Data Encryption Algorithms”, International Journal of Computer Science and Communication Vol. 2, No. 1, January-June 2011, pp. 125-127.

[6]. A. Siva Sankar, T. Jayachandra Prasad, M. N. Giri Prasad, "LSB Based Lossless Digital Image Watermarking using Polynomials in Spatial Domain for DRM", 2nd International Conference and workshop on Emerging Trends in Technology (ICWET) 2011 Proceedings published by International Journal of Computer Applications (IJCA).

[7]. Obaida Mohammad and Awad Al-Hazaimeh, "Hiding Data in Images Using New Random Technique", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 2, July 2012, ISSN (Online): 1694-0814.

[8]. Kh. Manglem Singh, S. Birendra Singh and L. Shyam Sundar Singh, "Hiding Encrypted Message in the Features of Images", IJCSNS International journal of Computer Science and Network Security, VOL.7 No.4, April 2007.

[9]. Mustafa Osman Ali and Rameshwar Rao, "Digital Image Watermarking Basics, and Hardware Implementation", International Journal of Modeling and Optimization, Vol. 2, No. 1, February 2012.

[10]. Pia Singh, "Image Encryption and Decryption Using Blowfish Algorithm in Matlab", International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013 ISSN 2229-5518.

[11]. Kahate, A. Cryptography and Network Security, Tata McGraw Hill Education Private Limited, NewDelhi. Second Ed. Ch 2, pp 38-59.

[12]. Neha Chauhan, Akhilesh A. Waoo and P. S Patheja, "Information hiding watermarking detection technique by PSNR and RGB intensity", Journal of Global Research in Computer Science, Volume 3, No. 9, September 2012.