ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

A Review on Image Steganography Techniques

Abhay Dakhole [1], Dr.Sanjay Badjate [2]

PG Student, Dept of Electronics, S.B.Jain Institute of Technology, Management and Research, Nagpur, India[1]

Vice Principal, S.B.Jain Institute of Technology, Management and Research, Nagpur, India [2]

Abstract: Image steganography is applicable in defence, police department, detective investigation department and medical field. In this paper we give a review on various techniques in image steganography. Nowadays internet technologies need a very strong level of security during data transmission. We can achieve it by steganography. Integer wavelet transform, list significant bit are some techniques used in image steganography. The results of such reviews of various methodologies are to get an efficient analogy to create a much better techniques for image steganography.

Keywords: Steganography, Cryptography. DWT, IWT.

I. INTRODUCTION

During confidential information exchange information security is very important. For achieving such purpose Steganography and cryptography are two ways. Steganography and cryptography are different from each other. The information is unintelligible in cryptography where as steganography hide the existence of the data. Cryptographic technique changes the data so that it cannot be understood but this generates curiosity. It would be more sensible if the secret data is cleverly embedded in other media so that nobody can guess about hidden data.

Steganography results in hiding of information by hiding confidential information within other information. Internet transactions over communication channel needs high security and confidentiality of transmitted sensitive information and it become a serious concern in information communication. Steganography as compared to cryptography secures communication between two parties by hiding the existence of the secret information rather than scrambling it. Steganography hides the secret data in unsuspecting cover media such as images, audio and video so that unauthorized persons do not realize that confidential data are being transmitted. Stego is the media that contains secret message. The focus of this paper is on hiding secret information in images.

The steganography is a Greek word formed from Steganos which means "covered" or "secret" and Grafia means "writing" or "drawing". In recent past Cryptography and steganography are used in data hiding and has received significant attention from industry and academia. Cryptography conceals the original data but steganography conceals the fact that data is hidden. High level of security has been provided by steganography. People widely use Steganography to secretly communicate information. For confidential information exchange information security is very important. Secret information exchange can be achieved by steganography and cryptography. Steganography differs from cryptography in various aspects. Due to a lack of strength in cryptographic systems a research has been driven in steganography.

Governments all over the world have created laws to either limit the strength of a cryptographic system or to prohibit it completely. Steganography has various applications in defence services, department of police, department of detective investigation, medical field etc. Businesses have also started to realize the importance of steganography in product information or communicating trade secrets. Avoiding communication through known channels reduces the risk of information being leaked. Hiding data in a photograph of the company picnic is less suspicious than communicating an encrypted file. To convey the data secretly by hiding the existence of data in some other medium such as image, audio or video is the main purpose of steganography.

Stenographic systems can be divided into two categories. In first existence of the data is kept secret and in second the existence of the data need not be secret. The main purpose of steganography is to communicate secretly and to avoid drawing attention to the transmission of hidden information Steganography is of three types Audio, Image and Video. Image steganography is the more famous than audio and video steganography.

II. RELATED WORK

Discrete Wavelet Transform converts discrete signal from the time domain into time frequency domain. The transformation product is nothing but set of coefficient organized in such a way that it enables spectrum analysis of the signal as well as spectral behaviour of the signal in time. The wavelet transform has emerged as a precious technology in the field of image compression. Wavelet-based coding provides improvements in picture quality at greater compression ratios. Fig. 1 shows the 2D DWT for image at various levels.

There are large numbers of steganography embedding techniques. These techniques modify the cover image with different methods. The main aim behind it is to hide the data at highest possible rate. Special domain embedding technique operates on the principal of tuning the parameter of the cover image so that the difference between the cover image and the stego image cannot be predicted by the human eyes.

Steganography generally exploit human perception because human eyes are not skilled to look for file which has hidden information inside them. Therefore steganography saves the data from people trying to hack them.

DOI 10.17148/IJARCCE.2015.4706

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

A. DWT

Discrete Wavelet Transform converts discrete signal from the time domain into time frequency domain. The transformation product is nothing but set of coefficient organized in such a way that it enables spectrum analysis of the signal as well as spectral behaviour of the signal in time. The wavelet transform has emerged as a precious technology in the field of image compression. Wavelet-based coding provides improvements in picture quality at greater compression ratios. Fig. 1 shows the 2D DWT for image at various levels.

When DWT is applied to an image it is divided into 4 sub bands: LL, HL, LH and HH. LL part contains the maximum information. So if the data is hidden in LL part the stego image can withstand compression or other manipulations. In the stego image distortion may be produced sometimes and then other sub bands can be used.

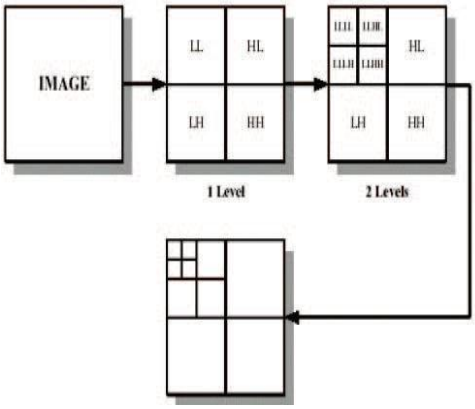

Figure 1: Two dimensional DWT

B. Insertion of Bit into the cover image

After values of b1, b2, b3, b4 has been received; these values are inserted into the cover image. These values are placed into the 2 bit LSB of the four consecutive pixels in cover image. The 2 LSB bits are replaced by 10,10,11,01 respectively by taking the pixels one by one from cover image

1	2	3	4	--	--	--	128	
110	241	33	97	--	--	--	--	1
186	--	--	--					2
--								3
--								4
--								--
								--
								--
								128

Figure 2. Cover Image (128 × 128)

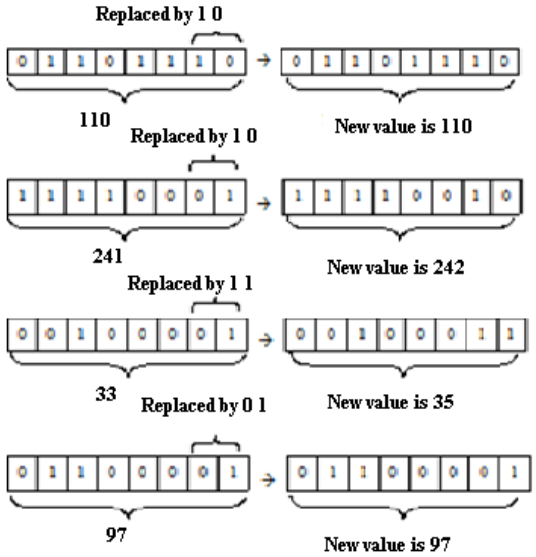

Figure 3. Insertion of Bit into Cover Image

C. Key Embedding using IWT

Using Integer Wavelet Transform the generated key is hidden in the cover image. In steganography, the cover image is not required at the receiver so once the secret data is extracted, some of the bit planes of the transformed coefficients of the cover image can be modified to hide the secret data. This increases the hiding capacity of the cover image. The middle bit planes of the higher frequency components of the transformed cover image are used to increase the robustness and security. Following are the steps to hide the key:

1) Take the integer wavelet transform (IWT) of the cover image.
2) Construct the binary image using the middle bit planes of the higher frequency components of the transformed image.
3) Compress the generated Key.
4) Now replace the middle bit planes of the higher frequency components of the transformed image by the bits of the compressed key.
5) Take the inverse Integer Wavelet Transform of the resulting image to get the stego image.

III.ALGORITHMS

A. Encoding Algorithm

Input: Take A gray level Secrete Image (m × n) and A gray Level Cover of size (2m × 2n);
Output: Stego Image of size (2m × 2n);

Steps:

1. Input eight pixel value of the secrete image and form block of 64 bits to the image encoding Function, which produces the encrypted secrete Image.
2. Divide the each pixel value of encrypted secrete image into 4 parts containing 2 bits each.
3. One by one insert these pixel values into the LSB position of first four pixels in the cover image.
4. End.

DOI 10.17148/IJARCCE.2015.4706

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 7, July 2015

B. Decoding Algorithm

Input: Take a Stego Image of size (2m × 2n);
Output: A gray level Secrete Image (m × n);

Steps:

1. Input each pixel value and take 2 bit LSB from 4 consecutive pixel value of the stego image.
2. Concatenated four 2bit LSB and get 8 bits of each pixel of encrypted secrete image.
3. Now taking eight consecutive pixel value form block of 64 bits are input to decoding Function (DES) using same parameter but keys value used in reverse order getting first eight pixel value of secrete image.
4. End.

C. Add With-Carry Generators

With a simple example we introduce add-with-carry generators. Consider the classical Fibonacci sequence. We take each element as a sum of the previous two. If we take this sequence mod 10, we have an example of a lagged-Fibonacci sequence with lags r=2 and s= land binary operation

VΔ W - V + W mod 1O

0,1,2,2,3,5,8,3,1,4,5,9,4,3,7, ...

The information description of the sequence is

$X_n = X_{n-2} + X_{n-1}$ mod 1O but to describe it and then define and then to establish its period we need the finite set X of 1 x2 vectors x = (x1, x2) with elements reduced residues of 10 and the iterating function f defined by f = (x1, x2) = (x2, x1+ mod m).Since f has an inverse , for any initial vector x Ɛ X the sequence.

x, f(x), f^2(x), f^3(x)... ….

Depending on the initial vector x there is a longest cycle of period 60 as well as shorter cycles of periods 1, 3,4,12 and 20. Every period is the least common multiple of the periods of moduli 2 and 5. Now let us consider add with carry version of this generator. Suppose we assign two initial values i.e. 0, 1 and an initial "carry bit",i.e. O. Then every new digit is the sum of the past two digits plus the carry bit. The result is taken mod 10 and the next carry bit set to 1 or 0 according to whether the sum exceeds 10 or not. Using a superscript to indicate the carry bit, the sequence of digits becomes

$0,1^0,1^0,2^0,3^0,5^0,8^0,3^1,2^1,6^0,8^0,4^1,8^0,3^1,4^1,3^1,8^0,1^1,0^1,2^0,$…….

Formally, we have a sequence of iterates

x,f(x),f^2 (x), ... but now our x come from the set X of 1 x3 vectors x = (x_1+x_2,c) with x1, x2 reduced residues of 10 and c then the "carry bit", 0 or 1. Then the iterating function f is

(X_2, X_1 + c, 0) if X_1+X_2 + c < 10

(X_2, X_1 + X_2 + C - 10,1) if X_1+X_2 + c ≥10

For initial vectors x = (x1,x2,0) with the sequence 0,1,1,2,3,5,8,13,21,34,55,89, ... ,

Xl < x20r X = (Xl,x2,1 with xl > x2)

of iterates x,f(x),f^2 (x) is strictly periodic with period 108. If the initial vector x is not (0, 0, 0) or (9,9,9) then the sequence f(x) is strictly periodic with period 108, but the "seed" vector x may not reappear in the sequence. For finding the period and assigning seed vectors for add-with-carry generators we develop some rules. The general add-with-carry generator has a base b , lags r and s with r>s,a seed vector x = x1 ,x_2 ..... x_rc with elements "digits" of the base b . Then the generated sequence is x, f(x),f^2(x), f^3 (x), ... with x

$f(x_1$ ..... ,x_r,c)=

(x2,….xr,xr+1-s+x1+c,0) if X_{r+1-s}+X_l+C<b

(x2,….xr,xr+1-s+x1+c-b,1) if X_{r+1-s}+X_l+C≥b

By choosing base b, lags r and s and seed vector x the generated sequence x f(x) f^2(x) ... will be periodic with period b^r+b^k-2 these generators have extremely long periods. For example, when b is near each 2^{32} base-b "digit" is a computer word, and with r around 20 or so, then periods of some 2^{640} are attainable at the cost of only r memory locations and simple computer arithmetic.

IV. EXPERIMENTAL RESULTS

To measure the quality of reconstruction of Loss compression peak to noise ratio (PSNR) is used.

For example in image compression a signal is the original data, and the noise is the error introduced by compression.

We can use secret images of size 256X256 with the proposed technique and 128X128 as the dimension for secret image. It takes an execution time of nearly 8 seconds. Proposed model is stronger Steganography technique because without knowing the secrete keys, S-box mapping function, the extraction of secrete image is impossible. Also quality of cover image is also not degrading due to variation in two LSB of each pixel which reflects only 0 – 3 difference pixel value.

REFERENCES

[1] Samir K Bandyopadhyay, Debnath Bhattacharyya,Debashis Ganguly, Swarnendu Mukherjee and Poulami Das, "A Tutorial Review on Steganography" (IC3–2008 UFL & JIITU, p. no. 105-114).

[2] V.Srinivasa rao, Dr P.Rajesh Kumar, G.V.H.Prasad,M.Prema Kumar, S.Ravichand, "Discrete Cosine Transform Vs Discrete Wavelet Transform: An Objective Comparison of Image Compression Techniques for JPEG Encoder", International Journal of Advanced Engineering & Applications, Jan. 2010.

[3] M. F. Tolba, M. A. Ghonemy, I. A. Taha,, A. S. Khalifa "Using Integer Wavelet Transforms in Colored Image-Stegnography", International Journal on Intelligent Cooperative Information Systems, Volume 4, July 2004, pp 75-85.

[4] Ahmed A. Abdelwahab and Lobna A. Hassaan, "A Discrete Wavelet Transform Based Technique For Image Data Hiding", 25th National Radio Science Conference, 2008.

[5] Neda Raftari and Amir Masoud Eftekhari Moghadam, "Digital Image Steganography Based on Integer Wavelet Transform and Assignment Algorithm", Sixth Asia Modelling Symposium, 2012, pp 87-92.

[6] Jasmin Cosic , Miroslav Bacai, " Steganography And Steganalysis Does Local web Site contain "Stego" Contain " , 52 th IEEE Trans.International Symposium ELMAR-2010, Zadar, Croatia 2009 ,pp 85 – 88.

[7] Zhang Yun-peng , Liu Wei " Digital Image Encryption Algorithm Based on chaos and improved DES ", System, man and Cybernatics ,SMC 2009 , IEEE International Conference 11-14 Oct 2009, pp 474- 479.

[8] J. Mielikainen, LSB Matching Revisited, IEEE Signal Process. Lett. 13 (5) (2006) 285-287N F. Johnson.

[9] Steganography tools. Available from:http://www.jjtc.com/Security/stegtools.htm 2005.

[10] M. M Amin, M. Salleh, S. Ibrahim, M.R.K atmin, And M . Z .I . Shamsuddin "Information Hiding Using Steganography" 4* National Conference on Telecommunication Technology Proceedings, Shah Alam,Malaysia, 2003.