International Journal of Engineering Inventions
ISSN: 2278-7461, www.ijeijournal.com
Volume 1, Issue 5 (September2012) PP: 04-09

Image Compression for Authentication & Integrity of Data Based on Discrete Wavelet Transform

Ms. Neha Patil[1], Prof. N. A. Dhawas[2]
Assistant Professor
[1]Department of Computer Engg. SCOE Khargar, Mumbai University
Head Of Department
[2]Department of Information Technology SIT, Lonawala, Pune University

Abstract—The process of encryption and message authentication code is conventionally considered as orthogonal security mechanism. The objective of message security mechanism is to validate data authentication, whereas encryption is used to deform the message to achieve data confidentiality. The digital signature and watermarking methods are used for image authentication. Digital signature encodes the signature in a file separate from the original image. Cryptographic algorithms have suggested several advantages over the traditional encryption algorithms such as high security, speed, reasonable computational overheads and computational power. The frequency-domain techniques mainly used for watermarking of the human visual system are better captured by the spectral coefficients. The transforms are broadly categorized in two ways (a) Discrete Cosine Transformation (DCT) (b) Discrete Wavelet Transformation (DWT). It is very difficult to explain all the methods so in this paper we concentrated on DWT. The proposed research work is the integration of message authentication code as well as encryption where the parameterized hash value of an encrypted image is designed to be same as the hash value of the parent unencrypted original image. The hash value will be computed without decrypting the original data. Therefore the authenticity can be proven without revealing the actual information. A digital watermark and signature method for image authentication using cryptography analysis is proposed. The digital signature created for the original image and apply watermark. Images are resized before transmission in the network. After digital signature and water marking an image, apply the encryption and decryption process to an image for the authentication. The encryption is used to securely transmit data in open networks for the encryption of an image using public key and decrypt that image using private key.

Keywords—Image Authentication, DWT, Integrity of Data.

I. OBJECTIVE

The main objective of our project work is multimedia encryption that aims at rendering the information unintelligible under the influence of a key. Encryption aims at removing the redundancy and the correlation of the data by scrambling it. In order to protect data privacy, images and videos need to be encrypted before being transmitted to the destination. Because the multimedia data such as videos form large streams of data, partial encryption that encrypts only some significant parts of the data is employed. Multimedia has some special requirements like perceptual security, efficiency, cryptographic security, format compliance and signal processing in the encrypted domain.

II. INTRODUCTION

Our existing system described in order to boost the data security, we focuses on the marriage of the two levels of security. Multimedia encryption and multimedia authentication schemes serve two different purposes but they can be merged together in one system to protect confidentiality and to check the authenticity of the data. It is indeed a very challenging problem but if we can integrate the two functionalities simultaneously, it will revolutionize the area of multimedia distribution. A commutative watermarking and encryption has been proposed that embeds watermark into the encrypted media directly, which avoids the decryption watermarking-encryption triples. The encryption and watermarking operations are done on the same data part. Commutative watermarking and encryption scheme is proposed for media data protection. In the scheme, the partial encryption algorithm is adopted to encrypt the significant part of media data, while some other part is watermarked. It has been reported that commutative schemes based on partitioning the data are vulnerable to replacement attacks. Since one data part is not encrypted, it leads to leakage of information and it is vulnerable to watermark attacks. Digital signature is a sort of Cryptography. Cryptography means keeping communications private. Its mainly used for the converting of the information is encryption and decryption. You can access the information without access key. The main process of the digital signature is similarly as the handwritten signature. It's like paper signature and it having the digital certificate using this verifies the identity. Watermarking is a sub-discipline of information hiding. It is the process of embedding information into a digital signal in a way that is difficult to remove. It's providing copyright protection for intellectual method that's in digital format. The cryptography is providing better mechanisms for information security. In this analysis to provide the public and private keys for recovery the original information.

III. METHODOLOGIES

3.1 Digital signature and Watermarking

Digital signature is a sort of Cryptography. Cryptography means keeping communication private. It deals with encryption, decryption and authentication.

3.1.1. Secret key or Symmetric Cryptography

In this processes sender and receiver massages have to know the similarly key for encryption and description of the image.

3.1.2Public key or Asymmetric Cryptography

Asymmetric Cryptography involves two related keys, one of which only the 'private key' and
Other is 'public key'.

3.1.3 Creation of Digital Signature

The creation of digital signature is done by getting the details from administrator, and the created signature is posted to the signature table and this is used by the certification authority. This is done by the certification authority and creates a personal identification to the person. This is carried out by using the **Digital Signature** Algorithm and the **Secure Hashing** algorithm. This digital signature provides a personalization.

3.1.4 Digital Signature Algorithm

(i) GLOBAL PUBLIC-KEY COMPONENTS

1. p = a prime number,
   where 2^(L-1) < p < 2^(L) for 512 = < L = <1024
   and L a multiple of 64

2. q = a prime divisor of p - 1,
   where 2159 < q < 2160

3. g = h^((p-1)/q) mod p,
   where h is any integer with 1 < h < p - 1
   such that h(p-1)/q mod P>1 (g has order q mod p).

(ii) THE USER'S PRIVATE KEY:

x = a randomly or pseudo randomly generated integer with 0 < x < q

(iii) USER'S PUBLIC KEY:

y = g^(x) mod p

(iv) USER'S PER-MESSAGE SECRET NUMBER:

k = a randomly or pseudo randomly generated integer with 0 < k < q

3.2 Watermarking Digital Signature

Digital image watermarking schemes mainly fall into two broad categories:

3.2.1 Spatial-domain techniques

The spatial –domain techniques consist of two categories, these are as follows:

a) Least-Significant Bit (LSB):

The given image contains pixels these pixels are indicated by the 8-bit sequence, the watermarks are linked two the last, bit of selected pixels of the original image. its used to hide the information and attackers could not destroy the information.

b) SSM-Modulation-Based Technique:

These technique are applied in the water marking algorithms with an linked information and attached to the original image with pseudo noise signal, it's modulated by the watermark.

3.2.2 Frequency-domain techniques

The frequency-domain techniques mainly used for watermarking of the human visual system are better captured by the spectral coefficients. The transforms are broadly categorized in two ways DCT and DWT.

(a) Discrete Cosine Transformation (DCT)
(b) Discrete Wavelet Transformation (DWT)

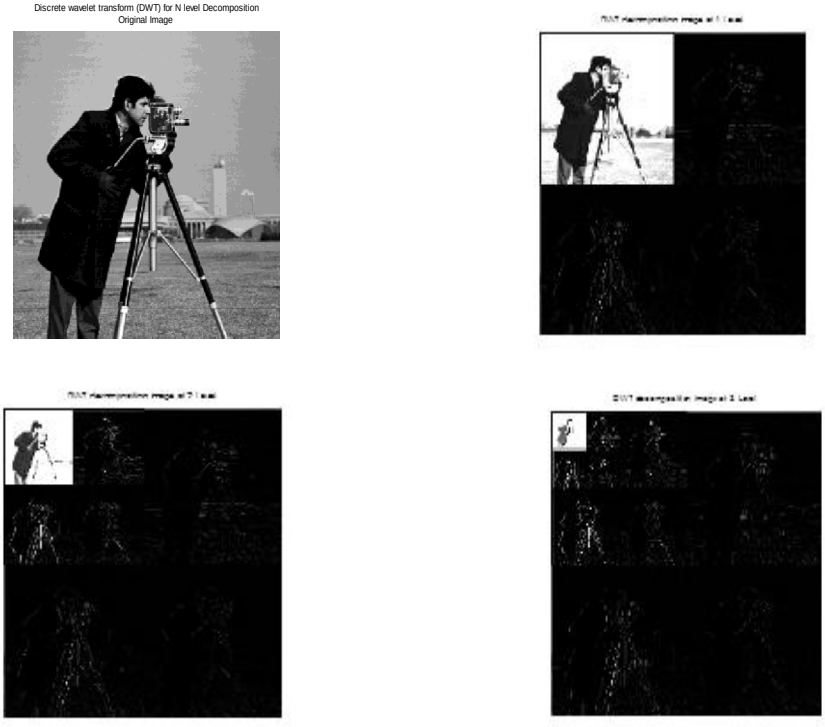
DWT is the method gives the correct result for analysis and compression of image. The wavelet transform preserves the time information along with frequency representation.

The **MATLAB program** is executed for different images & program is generalized to N number of levels. The program is given on next page:

```
%% Image processing based on discrete wavelet transform (DWT) for N level Decomposition %%
Clear all
clc
a=imread('cameraman.tif');%%size of image is 256*256
[NN MM]=size(a);
```

```
final=zeros(NN);%%Required for display of final image
a=double(a);
[row col]=size(a);
[Lo_D,Hi_D,Lo_R,Hi_R] = wfilters('db2');%%Daubechies-4wavelets
%%Lo_D stands for Low decomposition filter
%%Hi_D stands for High decomposition filter
%%Lo_R stands for Low reconstruction filter
%%Hi_R stands for High reconstruction filter
N=input('How many stages of decomposition you want N= : Type the value of N and press enter key')
figure(1)
imshow(uint8(a)),title({' Discrete wavelet transform (DWT) for N level Decomposition';'Original Image'})
for decomp=1:1:N %%Main loop for decomposition
for n=1:1:row
   b(n,:)=conv(a(n,:),Lo_D);%%convolving only the rows
   c(n,:)=conv(a(n,:),Hi_D);
end
for x=1:1:row
  for y=1:1:(col/2)
      B(x,y)=b(x,2*y);%%down sampling col
      C(x,y)=c(x,2*y);
  end
end
%%The size of B and C is N*n/2
[row col]=size(B);
for n=1:1:col
e(:,n)=conv(B(:,n).',Lo_D).';%%Convolving only the row%%
f(:,n)=conv(B(:,n).',Hi_D).';
g(:,n)=conv(C(:,n).',Lo_D).';
h(:,n)=conv(C(:,n).',Hi_D).';
end
E=0;F=0;G=0;H=0;
for x=1:1:row/2
   for y=1:1:col
      E(x,y)=e(2*x,y);%%downsampling the row
      F(x,y)=f(2*x,y);
      G(x,y)=g(2*x,y);
      H(x,y)=h(2*x,y);
   end
end
final(1:NN,1:NN)=[E F;G H];
%% The process can continue for further decomposition plotting
no=decomp+1              %%required to assign the figures(no)
figure(no)
imshow(uint8(final)),title(['DWT decomposition Image at ',int2str(no-1),' Level'])
[row col extra]=size(E);
a=E;
NN=NN/2;
b=zeros(row,col+3);
c=zeros(row,col+3);
B=zeros(row,col/2);
C=zeros(row,col/2);
e=zeros(row+3,col/2);
f=zeros(row+3,col/2);
g=zeros(row+3,col/2);
h=zeros(row+3,col/2);
end
```

After execution of program 4 images are displayed for N=3.
Given as follows:



The above process of 2-D discrete wavelet transforms are divided into three sub images for providing the watermarking for host image

3.2.3 Authentication using image verification

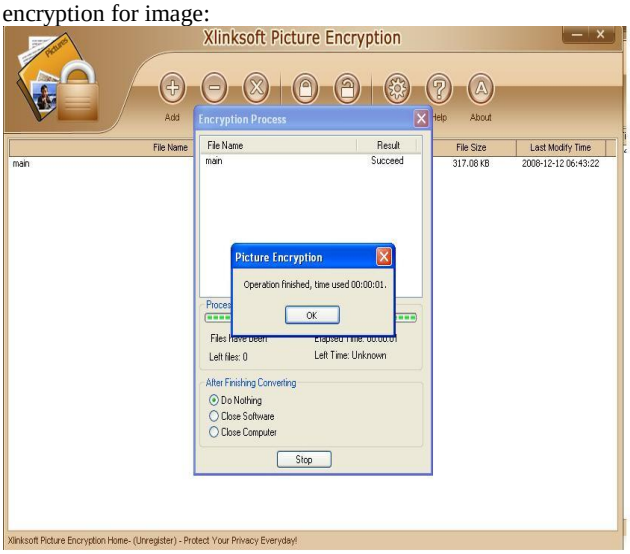
This is done by authentication verifier, initially he logins with person date of birth and document having signature like pan card, passport or driving license and extracts the signature. These details are submitted for the verification process. By this image verification is done and can know the detailed information of Water Marked image.

IV. CRYPTOGRAPHY

An encryption system is also called a cipher, or a cryptosystem. The message consists of plaintext, and cipher text. Denote the plaintext and the cipher text by P and C, respectively. The encryption procedure of a cipher can be described as C = EKe (P), where Ke is the encryption key and E is the encryption function. Similarly, the decryption procedure is P = DKd (C), where Kd is the decryption key and D is the decryption function. For public-key ciphers, the encryption key Ke is published, and the decryption key Kd is kept private, for which no additional secret channel is needed for key transfer.

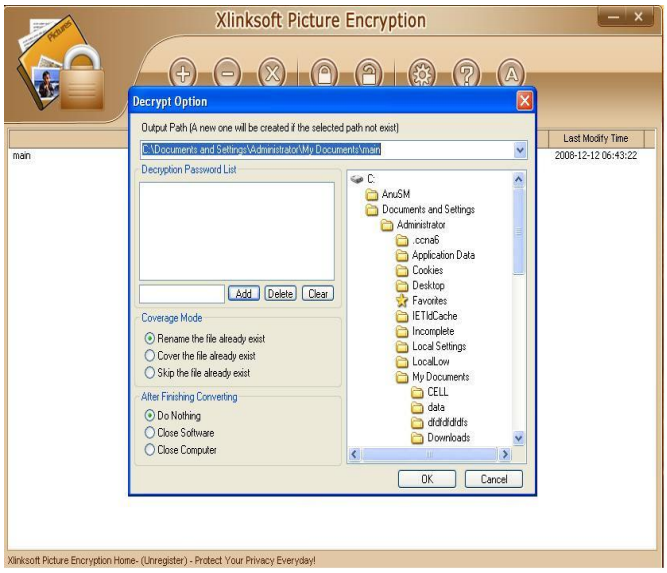
4.1 Encryption for image

The given picture shows the encryption for image:



4.2 Decryption for image

The given picture shows the decryption for image



V. CONCLUSION

In DWT method calculating wavelet coefficients at every pixel it generates lot of data. To reduce it we can use few pixels for analysis to get accurate readings. In wavelet decomposition the signal is separated using slow and fast components using pair of Finite Impulse Response (FIR) filter.

Digital signature and watermark are two techniques used for copyright protection and authentication, respectively. In this paper a digital signature and watermark methods are used cryptography analysis proposed for image security. Experiments show our scheme is robust to reasonable compression rate while preserving good image quality, and capable to authentication.

REFERENCES

1. G.L. Friedman, "The Trustworthy digital Camera: Restoring Credibility to the Photographic image", IEEE Transaction on Consumer Electronics, Vol. 39, No.4, 1993, pp. 905-910.

2. J. Cox, J. Killian, F.T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia", IEEE Transactions on Image Processing, Vol.6, No. 12, 1997, pp.1673-1678.

3. C.-Y. Lin and S.-F. Chang, "A Robust Image Authentication Method Distinguishing JPEG Compression from Malicious Manipulation", IEEE Transaction on Circuits and Systems of Video Technology, Vol. 11, No. 2, 2001, pp.153-168.

4. J. Fridrich, "Robust Bit Extraction from Images", in Proceedings of IEEE International Conference on Multimedia Computing and Systems (ICMCS'99), Vol. 2, 1999, pp. 536-540.

5. S. S. Maniccam, N. G. Bourbakis, Lossless image compression and encryption using SCAN", Pattern Recognition 34 (2001), 1229-1245

6. Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, "A new encription algorithm for image cryptosystems", The Journal of Systems and Software 58 (2001), 83-91

7. Jiun-In Guo, Jui-Cheng Yen, "A new mirror-like image encryption algorithm and its VLSI architecture", Department of Electronics Engineering National Lien-Ho College of Technology and Commerce, Miaoli, Taiwan, Republic of China.

8. Jui-Cheng Yen, Jiun-In Guo, "A new chaotic image encryption algorithm",Department of Electronics Engineering National Lien-HoCollege of Technology and Commerce, Miaoli, Taiwan Republic of China, E-mail: jcyen@mail.lctc.edu.tw

9. Shuqun Zhang and Mohammed A. Karim, Color image encryption using double random phase encoding", MICROWAVE AND OPTICALTECHNOLOGY LETTERS Vol. 21, No. 5, June 5,1999, 318-322

10. Young-Chang Hou, "Visual cryptography for color images", Pattern Recognition 36 (2003), www.elsevier.com/locate/patcog, 1619-1629

11. C. Yen and J. I. Guo, "A new image encryption algorithm and its VLSI architecture." In Proceedings of IEEE workshop on signal processing systems, pp. 430–437, 1999.

12. M. V. Droogenbroech, R. Benedett, "Techniques for a selective encryption of uncompressed and compressed images," In ACIVS'02, Ghent, Belgium. Proceedings of Advanced Concepts for Intelligent Vision Systems,2002.

13. [13] S. Changgui, B. Bharat, "An efficient MPEG videoencryption algorithm, " Proc e edings of the symposium on reliable distributed systems, 2002, page(s):708,711.

14. A. Mitra, , Y V. Subba Rao, and S. R. M. Prasnna, "A new image encryption approach using combinational permutation techniques," Journal of computer Science, vol. 1, no. 1, p.127, 2006, Available:http://www.enformatika.org

15. A. Sinha, K. Singh, "Image encryption by using fractional Four retransform and Jigsaw transform in image bit planes,"Source: optical engineering, spie-int society optical engineering, vol. 44, no. 5 , 2005, pp.15-18.

AUTHORS

Ms. Neha Patil is pursuing M.E. in Computer Engineering from Sinhgad Institute of Technology, Pune University and working as assistant professor in Saraswati College of Engineering Kharaghar. Her area of interest includes in Network Security, Image Processing, Artificial Intelligence and Neural network

Prof. N. A. Dhawas is the Head of IT Department at Sinhgad Institute of Technology, Lonawala, having experience of 15 years in the field of teaching. His research interest includes Mobile Computing, Image Processing, Applied Algorithms.