 ISBN: 978-81-927230-0-9

Digital Image Watermarking Using DCT for Image Authentication

Mohini Bankar

Computer Department, Savitribai Phule Pune University
SVPMCOE, Malegaon(Bk), Baramati, dist-Pune, Maharashtra, India
mohinibankar4@gmail.com

Sonal Choulang

Computer Department, Savitribai Phule Pune University
SVPMCOE, Malegaon(Bk), Baramati, dist-Pune, Maharashtra, India
sonalchoulang1@gmail.com

Sarika Pawar

Computer Department, Savitribai Phule Pune University
SVPMCOE, Malegaon(Bk), Baramati, dist-Pune, Maharashtra, India
sarikapawar8009@gmail.com

Trupti Nimbalkar

Computer Department, Savitribai Phule Pune University
SVPMCOE, Malegaon(Bk), Baramati, dist-Pune, Maharashtra, India
truptinimbalkar1@gmail.com

Prof S. A. Dabhade

Computer Department, Savitribai Phule Pune University
SVPMCOE, Malegaon(Bk), Baramati, dist-Pune, Maharashtra, India
saralapatil174@gmail.com

Abstract: As the need for information over network is high.therefore such Media files which are shared in networking sites and other areas must be highly protected to prevent files from hackers. Watermarking is a prevention technique used to prevent media files like images, audio and video files.The introduction of 3G wireless communication systems, together with the fast growing distribution of digital images and the growing interest on their originality initiates an sudden need of authenticating images received by fallible channels, such as public Internet and wireless networks. To meet this need, a content based image authentication scheme that is suitable for an insecure network and robust to prevent transmission errors is projected.In this scheme, multi-scale features are used to make digital signatures robust to prevent image degradations and key dependent parametric wavelet filters are engaged to improve the security against counterfeit attacks. This scheme is also able to characterize tampering areas in the attacked image. The information about the file encryption using Advance Encrypt Standard algorithm and watermarking using discrete cosine Transform Algorithm.

Keywords—Authentication,Digital Signature,Water Marking,Content authenticity verification, Error concealment, Embedding, Cryptography.

I. INTRODUCTION

Internet is a tremendous communicating channel. Because of the progress in networking and multimedia applications, multimedia contents can easily be attacked by the unauthorized persons. To confirm content integrity and to forbid duplication, image authentication method have been emerged. A secure digital signature scheme is one of the image authentication method that is suitable for an vulnerable environment,and is robust to transmission errors.In digital watermarking, a watermark is enclosed into a cover image in such a way that the consequent watermarked signal is robust to certain distortion caused by either standard data processing in a affable environment or malicious attacks in an unfriendly environment.

The system is proposed to provide authentication or security for digital media.In system we use Digital Watermarking image integrity to implement it we use Discrete Cosine Transform and for image encryption SHA Algorithm.A large number of networked multimedia applications have been created because of the advances in digital media technologies and networking. Those networked multimedia applications are often employed in a distributed wireless network environment that makes multimedia contents able to be attacked or harmed by the attackers. For insecure environments, it is possible for an

attacker to interfere with images without permission during transmission. To guarantee honesty and reliability, image authentication techniques have been introduced to confirm content integrity nothing but the quality of being honest,and prevent forgery.

II. LITERATURE SURVEY

Following are existing system description:.

A. *A robust content based digital signature for image authentication[8]*

Digital signature technique is used for image authentication ,but the problem with this scheme is that the signature is enclosed in image and hence the contents of original image get modified.

B. *Structural digital signature for image authentication: an incidental distortion resistant scheme*

A structural digital signature scheme is conferred but the parent child pairs make it more inclined to random changes in data, hence the system has more chances of being destroyed.

C. *Design of a robust and secure digital signature scheme for image authentication over wireless channels*

In this wavelet transforms are used to create signature, but the problems with wavelets are their high computational complexity, low security and robustness.

D. *secure and robust digital signature scheme for JPEG2000 image authentication*

A robust authentication can be accomplished at a cost of low security and also forfiet the image quality. Some other methods such as: distributed source coding and JPEG header can also give reliable results at the cost of system complexity.

III. SYSTEM ARCHITECTURE

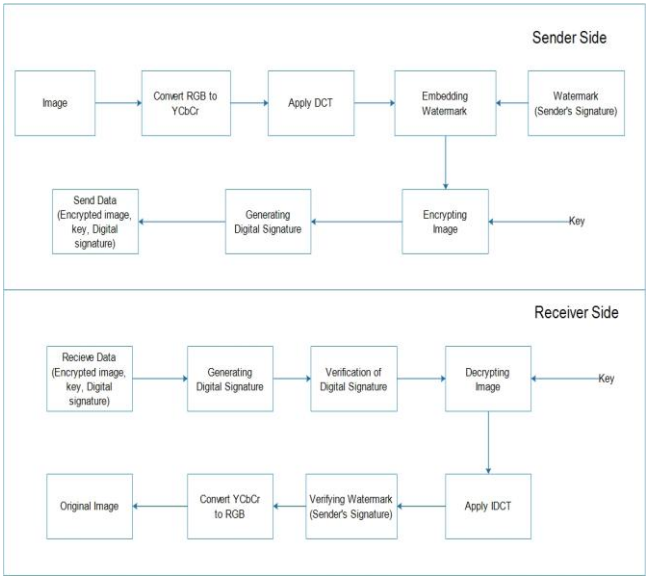

Fig. 1. System Architecture

- In our proposed system the input is original image on that original image the DCT(Discrete Cosine Transform)algorithm apply.That algorithm convert image into block.
- Firstly,we convert the image color RGB to the YCbCr .RGB colors are easilyvisible to human eye.But,the YCbCr color cannot view by human eye.
- YCbCr color space in that Y is the component that is the brightness,Cb component is the blue color minus Y component and the Cr means red color minus Y component.After converting YCbCr apply DCT.
- We select the one block for embedding watermark on that we embed the sender signature as a watermark.
- After embedding watermark this is encrypted at the sender side using sender private key
- for encrypting the image In that system we use AES(Advanced Encryption Standard)algorithm.
- For Providing the authentication on sender side on that image generate the digital signature for the authenticity using the DSA(Digital Signature Algorithm).
- After all that process the sender send the encrypted image,sender private key,digital signature are included image send the data to receiver.
- At receiver side receiver receive that encrypted image,key and digital signature on that data the generated signature is verify on that receiver side using the DSA algorithm After verifying that signature receiver decrypting the image using AES algorithm by using the receiver private key. on the decrypted image apply the IDCT(Inverse Discrete Cosine Transform) algorithm.
- IDCT is convert the image into spacial domain to frequency domain. then the verify that alternate at receiver side that watermark is the senders signature which we embedd in the image.
- then again the receiver convert the image color space YCbCr to the RGB to view the image constraints. then the receiver get the original image that image is in the form of encryped and that image having the authenticity and security
- In this project sender send the image to the receiver securely.

IV. ALGORITHM

1. DCT(Discrete cosine transform):

2D-DISCRETE COSINE TRANSFORM:

$$F(jk)=a(j)a(k)\sum_{m=0}^{N-1}\sum_{n=0}^{N-1}f(mn)\cos\left[\frac{(2m+1)j\pi}{2N}\right]\cos\left[\frac{(2n+1)k\pi}{2N}\right]$$

2D-IDCT:

$$f(mn)=\sum_{m=0}^{N-1}\sum_{n=0}^{N-1}a(j)a(k)F(jk)\cos\left[\frac{(2m+1)j\pi}{2N}\right]\cos\left[\frac{(2n+1)k\pi}{2N}\right]$$

A] WATERMARK EMBEDDING

The WATERMARK EMBEDDING steps using this technique are following:

1]Read colour host image.
2]Convert RGB to YCbCr components.
3]Apply DCT.
4]Embed the watermark components in to the frequency subcomponents .
5]Apply IDCT.
6]Convert YCbCr to RGB.
7]Get watermarked image
8]Check Authentication.

B] WATERMARK EXTRACTION

The WATERMARK EXTRACTION steps using this technique are following:

1]Read Watermarked image.
2]Convert RGB to YCbCr components
3]Apply DCT.
4]Extract the watermark components from frequency subcomponents .
5]Convert YCbCr to RGB.
6]Get watermark image
7]Check Authentication.

2.AES(Advance Encryption Standard)

1] Byte Substitution
2] Shift Row
3]Mix Column
4]Add Round Key

3.DSA (Digital Signature Algorithm):

1] Signing :

In Signing phase the user send the signature it is generated in the binary code at the sender side. This binary code is authenticated certificate uses in private key and binary code will be converted into the digital signature.

2] Verification :

In Verification phase the binary code will be decrypted using the senders private key at the receiver side. and this decrypt code and original code will be matched then the we conclude that the signature is verified.

4.SHA(Secure Hash Algorithm)

1]Padding:
Add Padding To the end of the original Image.
2]Append Length:
Appended to end of padding as a 64 bit block.
3]Divide:
Divide the input into 512 bit blocks Input message is now divided into block.
4]Initialize:
Initialize Chaining Variable There are five Chaining variable i.e A,B,C,D,E.

5]Process Block :
Here we consider single register for storing the temporary intermediate as well as final result

V. CONCLUSIONS

In this project we presented a new method of embedding watermark into colour image.The RGB image is converted to YCbCr and watermarked by using discrete cosine transform (DCT). The luminance component Y of image is considered for embedding watermark. The performance of the presented method can be assessed by PSNR,SNR,MSE and NC for RED,BLUE and GREEN. Existing techniques have worked on the gray scale of image, we have taken results for RED,BLUE and GREEN separately. Content-dependent structural image features and wavelet filter parameterization are incorporated into the traditional crypto signature scheme to enhance the system robustness and security. The secure digital signature scheme can achieve good robustness against transmission errors and some acceptable manipulation
operations.

ACKNOWLEDGMENT

It gives us great pleasure in presenting the preliminary project report on 'Digital Image Watermarking using DCT for Image Authenticatison'.we would like to take this opportunity to thank my internal guide Prof. Dabhade S.A. for giving me all the help and guidance we needed. We are really grateful to them for their kind support. Their valuable suggestions were very helpful.

We are also grateful to Prof. Mhaske V.D., Head of Computer Engineering Department,SVPM COE for her indispensable support, suggestions.

REFERENCES

1. Manpreet Singh, Harpreet Kaur ,Ajay Kakkar Dept. of E.C.E. Thapar University, Patiala, India "Digital Signature Verification Scheme for Image Authentication" 21-22nd December 2015.
2. QIBIN SUN and SHUIMING YE Institute for Infocomm Research, 21 Heng Mui Keng Terrace, 119613, Singapore "A CRYPTO SIGNATURE SCHEME FOR IMAGE AUTHENTICATION OVER WIRELESS CHANNEL" 23 December 2003.
3. Pravin M. Pithiya PG Student, Department of Electronics and Communication Engineering SPCE, Visnagar, Gujarat, India "DCT Based Digital Image Watermarking, De watermarking and Authentication" 3 May 2013.
4. Anjali Bhansali, HiralBarot, KinjalMasrani, Shraddha Shah, and Vicky Chheda "Encrypting Watermarked Images: A Transparent Approach" December 2013.
5. Manpreet Singh, Harpreet Kaur , Ajay Kakkar Thapar University, Patiala,India "Digital Signature Verification Scheme for Image Authentication" 22nd December 2015.
6. S. S. Sudha1 , K. K. Rahini Assistant Professor, Department of Computer Science, PSG College of Arts and Science, Coimbatore, India. " PREVENTION OF WATERMARKING ATTACKS USING CRYPTOGRAPHY METHOD" February 2014.
7. Samir Kumar Bandyopadhyay Dept. of Computer Sc. and Engg, University of Calcutta 92 A.P.C. Road, Kolkata 700009, India. "Invisible DigitalWatermarking Through Encryption" August 2010.
8. Qibin Sun, Shuiming Ye, Ching-Yung Lin and Shih-Fu Chang Institute for Infocomm Research, 21 Heng Mui Keng Terrace, 119613, Singapore. "A Crypto Signature Scheme for Image Authentication over Wireless Channel".