Digital Image Watermarking Based on LSB for RGB Image

Jesily Mol A[1] Poornima A V[2] Saranya U[3]
[1,2,3]Department of Technology in Computer Science
[1,2,3]Nehru College of Engineering and Research Centre Thrissur, India

Abstract— Due to the popularity of Social Networking applications and websites, the use of images as well as multimedia has been increased drastically. These file contents are transformed through open networks. The main challenges in open networks are lack of authentication, authorization and confidentiality. In order to preserve authentication, one of the popular mechanism is the use of copyright. By embedding copyright protection, we can ensure that the entities that take part in communication are authenticated. Our aim is to implement an efficient mechanism for copyright protection. In this paper, we use LBR algorithm to generate watermarked image. For enhancing Security, Secrecy Sharing Using parameters and Random Numbers are used in both client side.

Key words: RGB Image, Enhancing Security, Watermarking

I. INTRODUCTION

Now a days, various modes of communication like LAN, WAN and INTERNET are widely used for communicating information from one place to another around the globe. Such communication networks are open and any one can access easily. They are regularly monitored and an intercepted. So to prevent unauthorized use of digital content presently three main methods of information security is being used: watermarking, steganography and cryptography.

In watermarking, data are hidden to convey some information about the cover image such as ownership and copyright. Copyright is a legal right that an owner used to prove exclusive right for its use and distribution. One of the popular method of copyright protection is digital image watermarking. Digital watermarking is a process to embed some information called watermarking into the host image, which cannot be easily extracted by a third party. Digital watermarking is of two type, visible watermarking and invisible watermarking. Invisible digital watermarking is a type of data hiding that aims at covering information in a medium to prove authentication, integrity or provide additional information. Digital watermarks are inside the information so that the ownership of the information cannot be claimed by the third party. The efficient way of implementing digital image watermarking technique is LBR algorithm. The LBR algorithm embeds the watermark in the least significant bits of pixel values of the cover image (CVR). As the open networks are insecure we use Secrecy Sharing Using Parameters, for exchanging cryptographic keys over an open channel. To increase the security a pseudo random number is generated for each user. The user need to use the random number as a credential.

II. EXISTING SYSTEM

In the existing system, the color image is converted into grey scale image for embedding watermark. So the clarity of the image reduces and also visual quality degrades. The system does not check whether the communicating entities are one they claim to be and there is no validation of users.

III. PROPOSED SYSTEM

In proposed system, visual quality and clarity of the image increases because the watermark is embedded to the color image. In this system, the users are validated and check whether the communicating entities are one they claim to be by preserving authentication, copyright protection and integrity.

IV. IMPLEMENTATION

The proposed system can be implemented using PHP with Dream Weaver as front end and My SQL as back end.

The watermarking process begins with an encoder insert watermark into the cover image and produce the watermarked image. The decoder extracts and validates the presence of watermark. The watermark is a logo which contains some data like security and copyright information of host image. The watermarking process should contain and watermark embedder and extractor as shown in following figures.

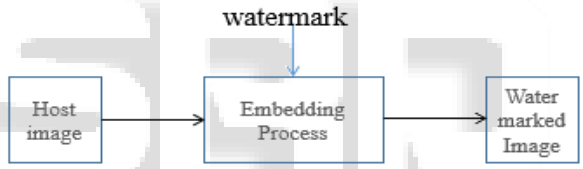

Fig. 1: Watermark embedder

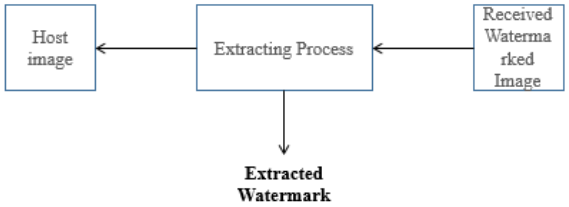

Fig. 2: Watermark extractor

The user have to first register on the site. After registering the admin will provide a secret key or pseudo random number that is to be used for sending and receiving process. Then the user can login with their username, password and pseudo random number as secret key generated at the time of registration. System will compare the secret key entered with the number generated at the time of registration. If it matches then the user will logged in. Then the user can chose the cover image and the secret image that he/she want to send. User must select a receiver and share a key using key exchange method. The user send the watermarked image to appropriate receiver by using least bit replacing algorithm (LBR).

At receiver side the watermark is extracted from the watermarked image by providing the credentials. Only the authenticated user can retrieve the secret information from cover image. The following figure illustrates the watermarking process.

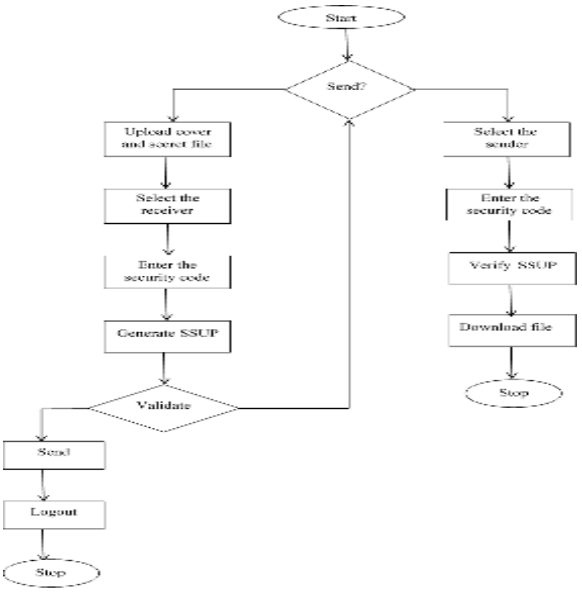

Fig. 3: Watermarking process

A. *Least Bit Replacement*

One of the most common techniques used in watermarking today is called least bit replacement (LBR). This method is exactly what it sounds like; the least significant bits of the cover-image are altered so that they form the embedded information. The following example shows how the letter A can be hidden in the first eight bytes of three pixels in a 24-bit image.

Pixels: (00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)
A: 10000001
Result: (00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

The three underlined bits are the only three bits that were actually altered. LBR insertion requires on average that only half the bits in an image be changed. Since the 8-bit letter A only requires eight bytes to hide it in, the ninth byte of the three pixels can be used to hide the next character of the hidden message.

B. *Secrecy Sharing Using Parameters*

This method is used for establishing shared secret key over an unsecured communication channel. Here, symmetric key cryptosystem is for sharing the key without communicating each other. The following figure shows the working of Secrecy Sharing Using Parameter.

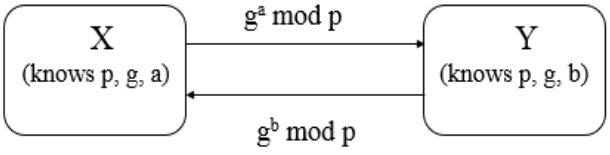

Fig. 4: Secrecy Sharing Using Parameter

C. *Random Number Generation*

Random Number Generation is an algorithm for generating a sequence of numbers whose properties approximate the properties of sequences of random numbers. The algorithm produces endless strings of single-digit numbers, usually in base 10, known as the decimal system. When large samples of pseudo-random numbers are taken, with equal frequency each of the 10 digits in the set{0,1,2,3,4,5,6,7,8,9} occurs even though they are not evenly distributed in the sequence.

V. RESULT AND DISCUSSION

Fig. 5: Home Page

The figure shows the home page. Here the user have to register first after that he/she can login using the username, password and the secret number.

Fig. 6: Sending Files

The figure shows Send File Page, in which the sender can send the secret file embedding it into the cover file to specified user. The user must provide security code which is generated at the time of registration. Sender will provide a number for key exchange. The sender can choose the file from upload files. First the cover file is choosen after that the secret file can be specified.

Fig. 7: Downloading Files

The figure shows the Download File Page, in which the receiver can select the sender and the file. The

receiver should enter the security code given at the time of registration and a value for key exchange. If the key generated at receiver side is equal to the key generated at sender side the secret file will be downloaded otherwise file cannot be downloaded.

VI. CONCLUSION

In the present world, the data transfers using internet is rapidly growing because it is so easier as well as faster to transfer the data to destination. So, many individuals and business people use to transfer business documents, important information using internet. Security is an important issue while transferring the data using internet because any unauthorized individual can hack the data and make it useless or obtain information. The proposed approach uses LBR technique to embed the secret image to cover image. A good balance between the security and the image quality is achieved. Thus, the computational complexity is reduced.

VII. FUTURE SCOPE

In future, digital watermarking can also be implemented in audio as well as video to provide the evidence of its authenticity. The security using Least Bit Replacement Algorithm is good but can improve the level to a certain extent by varying the carriers as well as using different keys for encryption and decryption. The future work on this project is to improve the compression ratio of the image. This project can be extended to a level such that it can be used for the different types of images like .bmp, .tif.

REFERENCES

[1] Rajni Verma and Archana Tiwari, "Copyright Protection for Watermark Image UsingLSB Algorithm in Colored Image", ISSN 2231-1297, Vol 4, No.5, pp. 499-506, October 2013.
[2] Babloo Saha and Shuchi Sharma, "Steganographic Techniques of Data Hiding using Digital Images", Defence Science Journal, Vol. 62, No.1, pp. 11-18,January 2012.

