ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING

National Conference on Advanced Innovation in Engineering and Technology (NCAIET-2015)

Alva's Institute of Engineering and Technology, Moodbidri

Vol. 3, Special Issue 1, April 2015

Two-Factor Authentication Approach for the Security of Highly Confidential Images

RAKSHITHA

Mtech in Computer Science, Shree Devi Institute of Technology, Kenjar, Mangalore, India

Abstract: This work proposes the novel scheme for two- factor authentication of confidential images using virtual watermarking technique. Here the content owner uses two images that is master image and sub image which are related to each other. In the first phase virtual watermarking is applied on both images and then the master image is encrypted using an encryption key. In the process of virtual watermarking we obtain a index array to which we will append encryption key used for the image encryption. In the next step index array will be compressed and encrypted using another encryption key. In the end encrypted image, encrypted array and encryption key used for the array encryption is transmitted to the receiver. In the receiver side the reverse process takes place and finally obtains the master image and the sub image back. Here the main focus is on lossless compression of the images, both the images are sent to the receiver without any distortion to the image and also receiver will receive the image without any data loss. This project is highly robust against any attacks due to virtual watermarking process because of which the attacker cannot retrieve the image easily.

Keywords: Virtual Watermarking, lossless compression.

I. INTRODUCTION

A digital watermark is a kind of marker that is embedded into digital signals such as audio or image data. It is mainly used to identify ownership of the copyright of such signal. "Watermarking" is the process of hiding digital information in a carrier signal, the hidden data does not need to contain any 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 mainly used for tracing copyright infringements and for banknote authentication.

In recent years, interest in digital watermarks has grown out of an increasing interest in intellectual property and copyright protection. Digital watermarks may be perceptible or imperceptible to human vision. Visible watermarks, by nature, are more intrusive to the media and act to deter theft of the media, such as a warning sign announces an alarm system even if one does not exist. Examples of such watermarks can be seen easily on most network television stations by the station's logo in the corner of the viewable screen. These watermarks are typically confined to an area of the image which is less intrusive to the overall image. Attackers have a visible target and can remove the watermark by cropping the image. Invisible watermarks have an advantage over visible watermarks, in that their location may be unknown.

A common practice is to distribute the watermark (or watermarks) across the entire image. This provides some protection against cropping attacks. However, the less perceptible a watermark is, it may be more vulnerable to manipulation. The purpose of digital watermarks is to provide copyright protection for intellectual property that is in digital format.

In recent years, many digital watermarking techniques have been proposed in the literature which is based on spatial domain technique and frequency domain technique.[1] In spatial domain technique the watermark is inserted in the cover image changing pixels or image characteristics. The algorithm should carefully weight the number of changed bits in the pixels against the possibility of the watermark becoming visible. In frequency domain technique the main target is to insert the watermarks in the spectral coefficients of the image. The most commonly used transforms are the Discrete Cosine Transform (DCT), Discrete Fourier Transform (DFT), and Discrete Wavelet Transform (DWT).

A. Spatial domaon techniques

Some of the spatial domain techniques are

1) *Least-Significant Bit (LSB):*

This is one of the earliest work of digital image watermarking schemes that embeds watermarks in the LSB of the pixels. Given an image with pixels, and each pixel being represented by an 8-bit sequence, the watermarks are embedded in the last (i.e., least significant), bit, of selected pixels of the image. This method is very easy to implement and does not generate serious distortion to the image.

Drawbacks of these methods are that it is not very robust against attacks. For instance, an attacker could simply randomize all LSBs, which effectively destroys the hidden information.

2) *SSM-Modulation-Based Technique*

Spread-spectrum techniques are methods in which energy generated at one or more discrete frequencies is deliberately spread or distributed in time or frequency domains. This is done for a variety of reasons, including the establishment of secure communications, increasing resistance to natural interference and jamming, and to prevent detection.

When applied to the context of image watermarking, SSM based watermarking algorithms embed information by linearly combining the host image with a small pseudo noise signal that is modulated by the embedded watermark.

B. *Frequency Domain Techniques*

Some of the frequency domain techniques are

1) *Discrete Cosine Transformation (DCT):*

DCT like a Fourier Transform, it represents data in terms of frequency space rather than an amplitude space. This is useful because that corresponds more to the way humans perceive light, so that the part that are not perceived can be identified and thrown away.

DCT based watermarking techniques are robust compared to spatial domain techniques. Such algorithms are robust against simple image processing operations like low pass filtering, brightness and contrast adjustment, blurring etc. Drawbacks of this technique is, they are difficult to implement and has high computational complexity.

2) *Discrete Wavelet Transformation (DWT):*

The Discrete Wavelet Transform (DWT) is currently used in a wide variety of signal processing applications, such as in audio and video compression, removal of noise in audio, and the simulation of wireless antenna distribution. Wavelets have their energy concentrated in time and are well suited for the analysis of transient, time-varying signals. Since most of the real life signals encountered are time varying in nature, the Wavelet Transform suits many applications very well.

Seperable reversible data hiding technique is used in this project , it means that data is recovered without any loss. In [2] Xinpeng Zhang proposed reversible data hiding on encrypted image here the image is encrypted and then a metadata is embedded to the image. Therefore it provides to levels of security once they have to use encryption key and once data hiding key. Drawback in such a approach is that while creating room for the data to embed there might be chances of loss of data. In [4] paper sheds light on the recent least-square(LS)-based adaptive prediction schemes for lossless compression of natural images. In [3] paper found a novel fact that by inserting the watermark using Least Significant Bit (LSB), the grey value of the image pixel either remains same or increases or decreases to one.

II. PROPOSED SCHEME

This paper proposes digital virtual watermarking technique, in which the image is not actually embedded into another image. The proposed method consists of retrieving every two bits of the sub image and compares it with the least significant bits of every bytes of the master image, If match is found store the index position of that pixel of master image together with and indicator to identify the color component, in an index array. Continue with the same process till it reaches the last pixel of the sub image. After this process encrypt the master image using one of the standard feedback shift register techniques. The initial value of the key sequence used for the encryption is appended to the index array. The index array is then compressed and encrypted using another key. The encrypted array, encrypted master image are sent to the receiver. The initial value used for the key sequence used to encrypt the index array is sent via one of the key exchange protocols.

This technique ensures that both the master image and sub image is not distorted and we are able to get back the image without any data loss. The receiver side gets the original image back without any loss of data.

Figure .1 shows the sketch for the data flow diagram of two-level authentication of highly confidential images.

A. *Sender Side*

The above flow diagram shows the two main components of the system. The sender side component consists of various modules. Sender side reads two images master image and sub image. Sub image is very confidential image whereas master image may contain metadata of the sub image. Sub image and master image are given virtual watermarking process where every two bits of the sub image is retrieved and compared with the least significant bits of the every bytes of the master image if match found then the index value of that byte of the master image is stored in an index array. Next the master image is encrypted via encryption key 1 using one of the standard feedback shift register technique. The encryption key 1 is appended to the index array and then the index array is encrypted via encryption key 2 again using one of the standard feedback shift register technique. Finally the encrypted image, encrypted index array and encryption key 2 is send to the receiver. The initial value used for the key sequence used to encrypt the index array is sent via one of the key exchange protocols.

In the sender side it is clearly shown two – levels of authentication provided to protect the sub image from any attacks.

Fig. 1. data flow diagram of two-level authentication of highly confidential images

B. *Receiver Side*

Once the receiver receives the encrypted master image, encrypted index array, and encryption key 2 he/she will decrypt the index image using encryption key 2. Now decompress the index array and retrieve back the appended encryption key 1 from it. Next step is to decrypt

DOI 10.17148/IJIREEICE

the image using encryption key 1, original master image is obtained. Once the index array and master image is retrieved, it has to undergo reverse virtual watermarking. In reverse virtual watermarking for every index value stored in the index array fetch the least significant two bits of that index and store in a integer array. Continue with the same process till the end of the index array is reached. Now the array to which the bits are stored are converted to the buffered image to obtain the original sub image. In this whole process it is noticed that nowhere the image data is lost. This is the advantage of using reversible virtual watermarking technique.

III. CONCLUSION AND FUTURE WORK

In this paper a novel scheme for hiding the images using virtual watermarking techniques and also lossless compression technique is used. The paper mainly focuses on providing bi-level security for highly confidential images due to which the system can provide more security for the images that gives very less chances of hacking the image. Here it is clear that even if the attacker gets the encrypted index array he will have no information of what data the index array hides in it and also how it is linked to the image, again if the attacker gets the encrypted master image he will have no clue as how to retrieve the sub image since the sub image is not embedded to the master image neither any information about sub image is stored in the master image. This is one of the main advantages that the virtual watermarking provides than comparing to usual watermarking techniques.

This can prove the robustness of this system any kind against attack. This system is assumed to be more secure than any of the watermarking technique since there is no screen for embedding images . Drawback of this project is that sub image should of small size and master image should be a good blend of RGB colur components to undergo vitual watermarking process without fail. The future work for this project can be that it can be still more improved by letting to accept any size sub image and also that master image may or may not be a good blend of RGB colors.

REFERENCES

[1] Keshav S Rawat, Dheerendra S Tomar ,"digital watermarking schemes for authorisation against copying or piracy against colour images" Indian Journal of Computer Science and Engineering Vol. 1 No. 4 295-300

[2] Xinpeng Zhang "Separable Reversible Data Hiding in Encrypted Image" ieee transactions on information forensics and security, vol. 7, no. 2, april 2012

[3] G.roslinenesakumari1, B. Vijayakumar2, L.Sumalatha3, and Dr V.V.Krishna4K. Elissa, "Secure and Robust Digital Watermarking on Grey Level Images," International Journal of Advanced Science and Technology Vol. 11, October, 2009

[4] Xin li, Michael T Orchard " Edge-directed prediction of lossless compression of natural images" ieee transactions on image processing, vol. 10, no. 6, june 2001

[5] Y. Shantikumar Singh1, B. Pushpa Devi2, and Kh. Manglem Singh3 ," A Review of Different Techniques on Digital Image Watermarking Scheme" International Journal of Engineering Research.

[6] Pooja Mishra, Biju Thankachan "A survey on various encryption and key selction techniques" International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 7, January 2013.