IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 3, Ver. VI (May-Jun. 2016), PP 37-41
www.iosrjournals.org

Virtual Watermarking for Color images

Ms. Rakshitha[1], Ms. Sharanya P.S[2]
[1]*(Computer Science, Vivekananda College of Engineering & Technology, India)*
[2]*(Computer Science, Vivekananda College of Engineering & Technology, India)*

Abstract: *This work proposes a virtual watermarking technique for colored images. In the proposed work, sender uses two images one is cover image and other is secret image. Let us consider the secret image to be embedded as sub image and the cover image as master image. The master image is chosen such that it is common to both sender and receiver such as Lena image which is used in most of the image processing projects. In the first phase of the project an index array is derived by applying virtual watermarking process on both master and sub image. Once the index array is obtained, the same is encrypted using an encryption key. The encrypted index array along with the encryption key is sent to the receiver. In the second phase, the receiver side decrypts the index array using the key. Once the index array is obtained reverse virtual watermarking is applied on index array and common master image. At the end of this process the original sub image is obtained back. The main advantage of this technique is that master image is not transmitted, hence providing more protection against image processing attacks.*

Keywords: *Index array, Key exchange protocol, Master image, Sub image, Virtual watermarking process.*

I. Introduction

Multimedia security is of highly significant concern for the internet technology due to the ease of duplication, distribution and manipulation of the multimedia data. Watermarking is one of the technologies that are widely used for the security of the multimedia data. One of the major aspect of watermarking is to robustness to various attacks, security and invisibility .Watermarking is nothing but hiding digital information in a carrier signal.

Digital Image watermarking is a technique that is used to hide or insert a digital signal or pattern into a digital image. This technique hides the crucial information present in the original data for protection from illegal duplication and distribution of multimedia data.

Effective digital watermarking must satisfy the following features. They are as follows:

- Imperceptibility– Watermarking should be done such a way that it should be invisible to the human eyes. Meanwhile the care should be taken that data quality is not degraded, and also that it should prevent attackers from finding and deleting it. Watermarking is called imperceptible if the watermarked content is equivalent to the original, un-watermarked content.
- Readily Extractable– The data owner or any control authority should be able to extract the watermark easily.
- Unambiguous – The watermark retrieval should unambiguously identify the data owner.
- Robustness– Watermarking should be such that it should able to tolerate some of the image processing attacks. Watermarking technique is also said to be robust if it is able to tolerate some class of transformation.

Digital watermarking is of two types one is visible and other is invisible watermarking. In visible watermarking the watermark is woven into the cover image, this watermark is visible to the human eyes. In case of invisible watermarking the watermark is not visible to the human eye, in this case watermark is embedded to the cover image either by inserting the watermark into some selected pixel positions, frequency co-efficient and so on. Our main focus in this paper is on invisible watermarking. In the rest of the paper we will refer cover image as master image and embedding image or secret image as sub image. In invisible watermarking the watermark is hidden into the master image and when this image is brought into internet there are high chances of altering the image by either changing the bits of pixels or changing the pixel position, because of which the entire master image is distorted and thus it becomes impossible to retrieve the sub image back. To avoid this, various invisible watermarking techniques were proposed. Let us go through some of the existing watermarking techniques. An Improved Invisible Watermarking Technique for Image Authentication is proposed in paper [1] in which the watermark is generated from pixel value of original image therefore there is no need of external image or logo. A survey on wavelet watermarking techniques and frequency watermarking techniques has been done in paper [2]. In third paper [3] a novel approach of inserting the watermark based on their grey level values and coordinate positions is being discussed. Paper [4] in reference list showed review on watermarking and its techniques, and also properties of watermarking and applications of various watermarking techniques. In paper

[5], a novel scheme for separable reversible data hiding in encrypted images. In this scheme the content owner encrypts the image using image encryption key and then hiding data into it using data hiding key. With an encrypted image containing additional data, if a receiver has the data-hiding key, he can extract the additional data though he does not know the image content. If the receiver has the encryption key, he can decrypt the received data to obtain an image similar to the original one, but cannot extract the additional data. If the receiver has both the data-hiding key and the encryption key, he can extract the additional data and recover the original content without any error by exploiting the spatial correlation in natural image when the amount of additional data is not too large. In sixth paper of reference list author has discussed about the spatial domain technique and frequency domain technique and also showed the measure of robustness of the watermarking techniques.

In all the above watermarking techniques we have found that sub image is embedded to master image. In all of these cases the master image is sent to receiver via internet, even though the existing techniques are robust against some of the watermarking techniques, there may be chances that the attacker modifies the pattern of the image either by changing the pixel values or frequency coefficients, then there is no way to extract sub image back completely. So this paper proposes a virtual watermarking technique in which the master image is not sent to the receiver via internet. Here we have used the common image as master image therefore there is no fear of attacker attacking the master image.

II. Proposed System

This paper proposes a virtual watermarking technique in which the master image is selected in such a way that it remains common to both sender and receiver. In this technique sub image is not actually embedded to the master image instead the information of the master image is used to embed sub image virtually to the master image. During this process we have used an extra data component that is Index array. The virtual watermarking process as follows , at first every two bits of the sub image is compared with every two bits of the master image if match found then, store the index position of the bit position of the matched bits in the master image. Repeat the same process till all the sub image bits are covered. In order to impose security the index array will be compressed and encrypted using any of the encryption algorithms and sent to the receiver. The key used for the encryption will be sent to the receiver separately via key exchange protocol. The master image is just used to obtain the watermark information but will not be brought into internet since the master image taken is a common image known to both the parties.

In this method we can see that virtual watermarking did not alter the master image and also that master image is not sent to the receiver which avoids image processing attacks. Fig.1 shows virtual watermarking process.

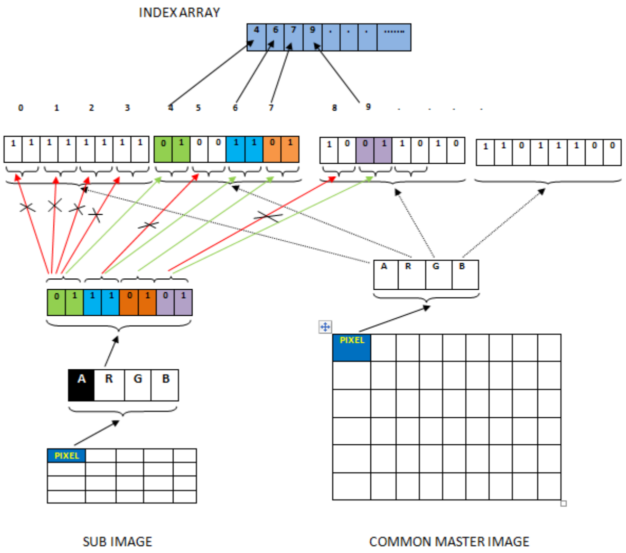

Figure.1 virtual watermarking process.

The above figure depicts virtual watermarking process, where the data for the embedding sub image on master image is obtained by fetching the information from master image as follows, Every two bits of the sub image is compared with every two bits of the master image, if match is found then the index position of the matched bit position of the master image is stored in Index array. Therefore the final outcome of the process is index array.

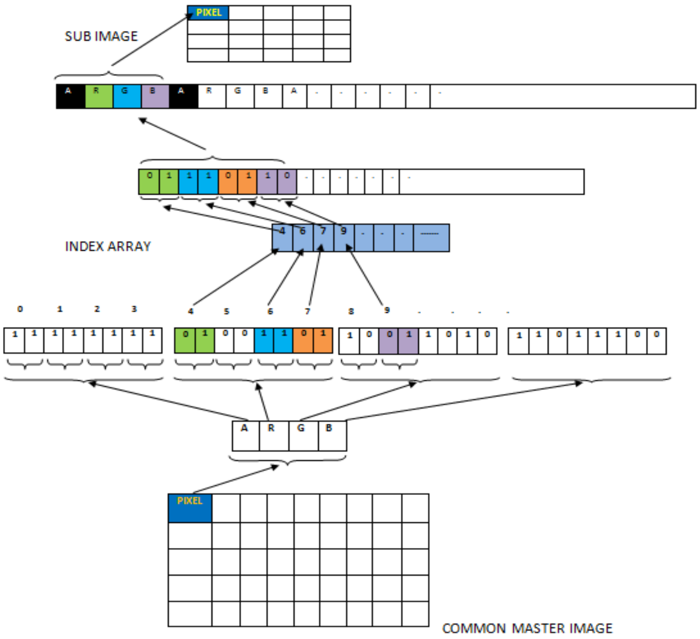

Figure.2 Reverse virtual watermarking.

Fig.2 shows reverse virtual watermarking process which will take place in receiver side. The receiver will have index array and also master image which is common to both sender and receiver, the reverse virtual watermarking is applied on these two images to obtain sub image back. The reverse virtual watermarking process is as follows: In the first step, bit positions stored in the index array are read and the matching bit positions values are fetched from the master image and stored in an array. Repeat the same process till the end of the index array is reached, once watermark values are fetched and stored in the array the array is converted to image. The final image obtained is nothing but the sub image.

Fig.3 shows data flow diagram of virtual watermarking system. This system consists of two components i.e. Sender side and Receiver side; the functions of these components are as follows:

A. Sender Side

In the sender side, the owner consists of sub image and master image, the master image is chosen such that it is common to both sender and receiver. Virtual watermarking is applied on master image and sub image and in the end of this process an index array is obtained. The index array is compressed and then encrypted using encryption key and send to the receiver meanwhile the encryption key is sent to the receiver via key exchange protocol. Below is the sender side algorithm.

Step 1: Read Sub image and master image.
Step 2: Create index array.
Step 3: For every two bits of the sub image.
Compare it with every two bits of master image.
If match found.
Store index position of the matched bits position of the master image in Index Array.
Continue till every bits of the sub image is covered.
Step 4: Encrypt index array using encryption key.
Step 5: Send encrypted index array to the receiver also encryption key via key exchange protocol.

B. Receiver Side

Receiver side initially consists of encrypted index array, decryption key and common master image. In the first step the receiver decrypts index array using encryption key, once the original index array is obtained reverse virtual watermarking is applied on master image and index array and sub image is obtained back without any loss in data.

Receiver side algorithm is as follows:
Step 1: Read encrypted index array, encryption key and common master image.
Step 2: Decrypt index array using encryption key.
Step 3: For every index values stored in the index array.

Retrieve two bits from the matched index from master image.
Store fetched two bits into a sub image array.
Step 4: Convert the sub image array to image, original sub image is obtained.

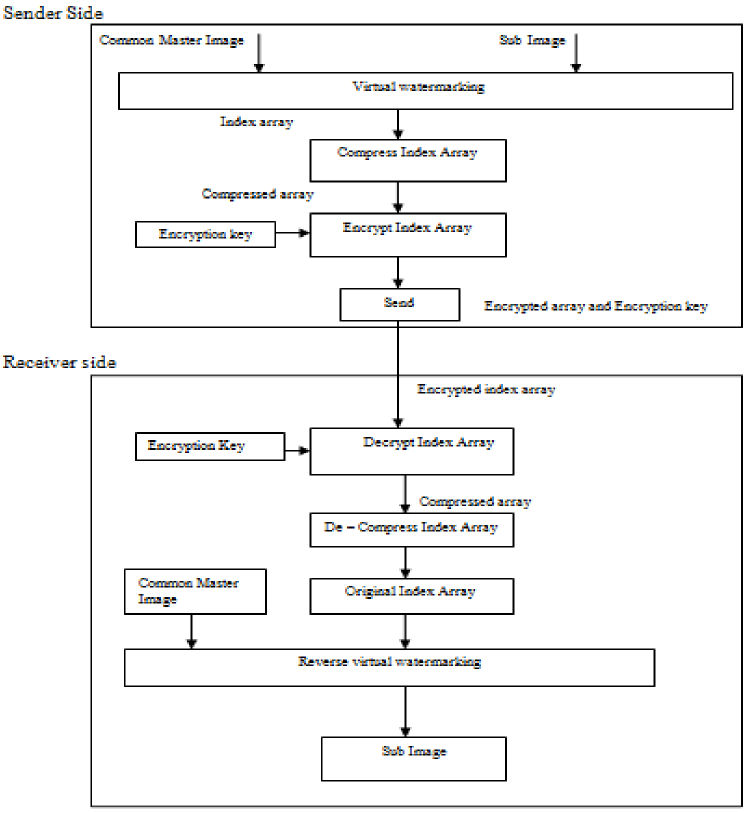

Figure.3 Data flow diagram of virtual watermarking system.

III. Experimental Results

The experiment is conducted in Java platform using NetBeans IDE. For experimental purpose we have considered master image as lena.png image of size 512×512 which is used in most of the image processing projects and Sub image as X-ray.jpg image which is three times smaller than master image. In this project we consider sub image should be three times smaller than master image. Fig.4 shows master image that is lena.png image. Fig.5 shows sub image that is X-ray.jpg image.

During virtual watermarking process master image is not altered to obtain index array. The similarity measurement between original watermark (sub image) and extracted watermark is obtained through Normalized Correlation (NC) coefficient and Accuracy Rate (AR).

Figure.4 Master image.

Figure. 5 Sub image.

A. Normalised Correlation (NC)

The Normalized correlation Coordinate (NC) computes the similarity measurement of original watermark and extracted watermark, which is defined as

$$NC = \frac{\sum_{i=1}^{N} \sum_{j=1}^{N} W(i,j) * W(i,j)}{\sum_{i=1}^{N} \sum_{j=1}^{N} W^2(i,j)}$$

Where N×N is the size of the watermark, W(i,j) and W^2 (i , j) represents the watermark and recovered watermark images. In this experiment we have found that NC will be equal to 1, since the original watermark and recovered watermark are found to be same.

B. Accuracy Rate (AR)

The accuracy rate (AR) is used to measure the difference between the original watermark and recovered one. AR is computed as follows:

$$AR = CP/NP$$

Where NP is the number of pixels in the original watermark and CP is the number of correct pixels obtained by comparing pixels of the original watermark to the corresponding ones of the recovered watermark. In this project the accuracy rate is also one.

Thus from the above results we can say that proposed virtual watermarking proves to be more secure comparing to any other watermarking techniques.

IV. Conclusion

This paper proposes a virtual watermarking technique in which the master image is taken as a common image and hence there is no need of sending master image to the receiver via internet. Disadvantage of this project is that we have to choose master image which is three times bigger than sub image to obtain better results. This disadvantage can be taken as a future work and a better virtual watermarking technique can be proposed to enhance robustness of the watermarking.

References

[1] Dhruv Arya, 2010 : *A Survey of Frequency and Wavelet Domain Digital Watermarking Techniques*, International Journal of Scientific & Engineering Research, Vol. 1, Issue 2.

[2] Dr. M. Mohamed Sathik, S. S. Sujatha, 2010 : *An Improved Invisible Watermarking Technique for Image Authentication* , International Journal of Advanced Science and Technology, vol. 24.

[3] G. Rosline Nesa Kumari, B. VijayaKumar, L. Sumalatha, Dr V.V. Krishna, 2009 : *Secure and Robust Watermarking on Grey Level Images,* International Journal of Advanced Science and Technology, Vol. 11.

[4] Keshav S Rawat, Dheerendra S Tomar, *Digital Watermarking Schemes for Authorization Against Copying or Piracy of Color Images*, Indian Journal of Computer Science and Engineering, Vol. 1 No. 4 295-300.

[5] Vinita Gupta, Mr. Atul Barve, 2014 : *A Review on Image Watermarking and Its Techniques*, International journal of Advanced Research in Computer Science and Software Engineering, Vol. 4.

[6] Xinpeng Zhang, 2012 : *Seperable Reversible Data Hiding in Encrypted Image*, IEEE Transactions on Information Forensics and Security, vol. 7, no. 2.