Survey paper on Copyright Protection for Images on Mobile Devices

Ashwini Suryawanshi
Information Technology
Pune University
ashsuryawanshi23@gmail.com

Shraddha Newase
Information Technology
Pune University
shraddhanewase@gmail.com

Minal Chachare
Information Technology
Pune University
minal.chachare@gmail.com

Sheetal Dudhane
Information Technology
Pune University
dudhane.sheetal9@gmail.com

***Abstract*— The upcoming era of mobile technology has also raised by sharing of images and other graphical data. With this protection to such files is also plays a vital role. Using watermarking we can guarantee to provide the ownership for these shared images. There are various techniques to provide digital watermarking introduced by different inventors. The results of these existing techniques are quite well but the unification of these techniques can be a better solution.**

***Keywords*—** Digital watermarking, Digital signature, Steganography ,DCT with LSB, DWT.

I. INTRODUCTION

Behind various graphical images the textual information can be covered in such a way that the unauthorized user is unable to access, such term is framed as data hiding. To provide proper authentication for data hiding process following techniques are enlisted :-

- Steganography
- Cryptography
- Digital signature

Stegnography: Stegnography is the science of hiding the data behind the images. Such encoding is done by sender which the respectedreceiver only can decode and extract the data.Stegnography consists open code which hides information in an appropriate carrier message and receives covert communication [1]. Though such secure communication stegnography does not guarantee to provide confidentianality to the communication. This drawback is overcome by next technique.

Cryptography: Cryptography is termed as process of converting plain text into the cipher text. For acquiring such conversion two types of keys are used which are public key and private key. Public key is used for encrypting and decrypting the data and is known to every communicator over network. Every communicator has its own private key and public key which is used for decrypting the encrypting data only [2]. Thus, cryptography helps to provide confidentionality, data integrity, authentication and non-repudiation of data [3]. To enhance cryptography another techniques are emerged.

Digital signature: Digital signature is a structure of sending the message from one user to another in secure manner as sender encrypts the message by using its private key over network to the receiver. Now receiver decrypts this message by using its private key only if he is aware of sender public key. Digital signature strengths original authentication and content integration services.[3]

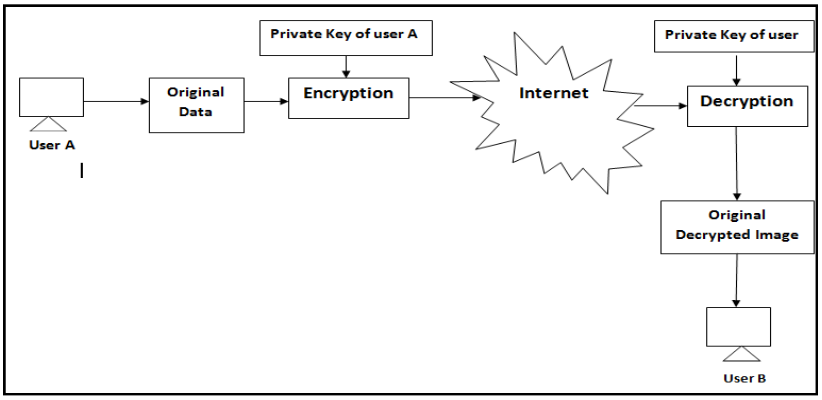

Fig. Digital signature

Digital Watermarking

Digital watermarking is the technique which contains the hidden information into the digital contents (image, videos, etc). It is the data where textual code is embedded over pictorial data or videos.

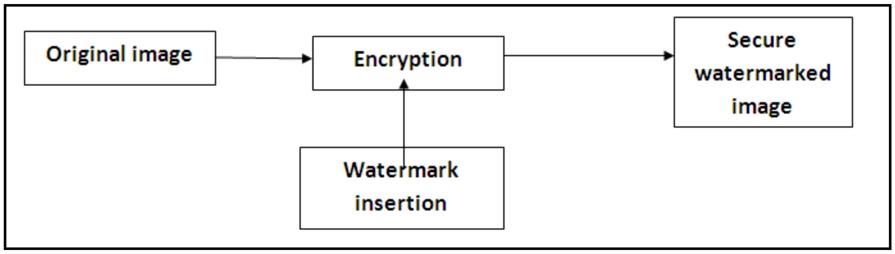

Fig. Digital watermarking

Digital watermarking consists of the following types:-

- Visible watermarking
- Invisible watermarking

- **Visible watermarking**: In visible watermarking the text or string inserted to the image is in the form of watermark and it is quite visible. These watermarked texts are generally logos that are embedded over another picture [1][2]. Basically the idea behind the visible watermarking technique is that it converts the text which is watermark over a bitmap image. Then it merges the text and the image by selecting the random pixels of the image [2]. The selection of these random pixels is totally dependent on the characters that are repeated in the watermarked string.

Generally, visible watermarking provides one sort of authentication to the image owner because if any other user attempts to remove the watermarked string from image then the quality of the image is degraded which reveals that the image is accessed in an unauthorized manner. Thus in visible watermarking image and the watermarked string both are visible to the user.

- **Invisible watermarking**: While the process of watermarking modification is done in some part of multimedia data which is included in invisible watermarking. The watermarked text is not visual to the unauthorized user. Images are broken into number of blocks. These blocks consists of number of pixels. In invisible watermarking these pixels are altered to embed the string over that image. By common image processing techniques the block that altered may be destroyed.The second category states the content or the string is protected. In this category images is validated but its representation is rejected by validation. Invisible watermarking is used for image verification in some terms[4].

II. Few Recently Invented techniques of digital watermarking.

2.1 Discrete Cosine Transform (DCT)

DCT is two dimensional in nature. The DCT technique accepts an image which is then divided into various frequency bands and is much for embedding string over image into middle frequency band [4]. Thus DCT domain watermark can work against the details such as filtering and noising.

Steps of DCT:-

→ RGB (Red-Blue-Green) color of the original image translated to creation of gray code.
→ The image is divided into 8X8 blocks by JPEG standards.
→ Now this 8X8 blocks are translated into cosine frequency domain.

Now extracting the watermarking image perform DCT execution on the original image and watermarked image. Then deduct our original image from the watermarked image and multiplying the extracted watermarked.

2.2 Discrete Wavelength Transform(DWT)

DWT is in one-dimensional in nature. In DWT technique the signal is categorized into two parts namely high frequency and low frequency. The edge component of the signal is the part of high frequency. Further low frequency is again divided into two parts that is high frequency and low frequency. This process is continuously carried out to be determined by the application.

Steps of DWT:-

→ Encoder: In first level the image is divided into four frequency bands using resolution. In second level the image is divided into seven frequency bands using resolution. In third level the image is divided into ten frequency bands using resolution. This process is kept on going for encoding.

→ Adding : Add pseudo-random sequence.

→ The normal distribution of an image is carried out using two relations mainly between watermarked image and the original image.

→ Now by refereeing these two relations among the watermarked image and the original image these relations are different but the goal of both the relations is same which is to watermark inserted over high value image coefficients.

By the help of DWT the edges and the textures are usually to the high frequency of sub-bands.

2.3 Singular value decomposition(SVD)

A new robust method is performed or executed by using the modification on singular value decomposition of image in CWT domain. Singular value decomposition is the technique which is used in linear algebra technique. Further linear algebra technique is used in variety of applications.

The additional use of Singular value decomposition technique is robustness against the most of the common attacks. Singular value decomposition is applied on image matrix in watermarking. In this the term watermark is obtained by altering the singular values in image matrix.

Modification of the Singular value decomposition technique is the widest or expandable technique in discrete wavelength transform (DWT) technique. Singular value decomposition is the optimal matrix decomposition in a least square sense package there is possible to have maximum signal energy in to various co-efficient. The main idea behind this technique is that if we embed the singular values in CWT then in order to use the properties of the frequency domain and Singular value decomposition simultaneously.

2.4 Least Significant Bit

In digital watermarking one of the technique uses the two dimensional array of pixels of an image in a container. This container is used to store the covered information using the least significant bit method.

By the human eyes it is difficult to predict the difference between the color of image. Taking this advantage execution of LSB on an image's color will not be predictable.

Steps of LSB :-

→ Convert the RGB standards of one image into gray scale image.

→ Perform repeated process of obtaining accuracy in image.

→ In watermarked image shift the most significant bit to LSB.

→ Assign zero to LSB of the host image.

→ Now insert step 3 of watermarked image to step 4 host image.

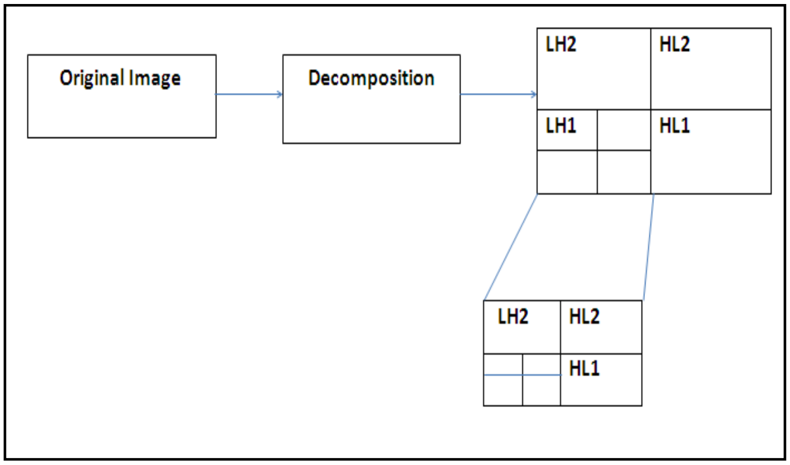

Fig. Least Significant Bit (LSB)

2.5 Code Division Multiple Access

Now a day there are different types of techniques is used for the digital image watermarking such as DWT, DCT, LSB but more flexible and secure technique is the CDMA technology.

CDMA is very secure technique in which encoded copyright message are embedded into original image by using the discrete wavelet transformation. The CDMA technique is used in spread spectrum technique and in that technique multiple users share the same frequency band at time[11].

The main purpose or the execution of this technique is to not allocate or assigns the separate frequency to the each users. In CDMA technique, watermark insertion is done and they includes 64 watermark sequences that is {A1,A2,……,A64} and this sequences is embedded into the 4X4 blocks into the quadrants, each blocks are 1024 blocks and in each blocks is only 32 blocks will be embedded and secret key is used to select the 32 blocks in quadrants.

By using DWT the process of watermark detection and retrieval is carried out. In this process received watermark image is decomposed into 1-level of quadrants. The secrete key that was used in the embedding this retrieval process is also used to define the 4x4 DWT coefficient blocks in the quadrants and they contain the hidden watermark bits.

CONCLUSION

The digital watermarking is highly used to provide secrecy to the graphical contents. In the existing systems retrieving encrypted data is possible but by using above mentioned techniques extracting data have became quite easy. In this digital technique authentication is provided to the images and ownership is also maintained.

Undoubtedly the techniques discussed above are extremely useful, a next step in this path would be to compare and evaluate all these various mechanisms by creating sets of data and an experimental test bed or to come upwith a collaborative approach to find more efficient solution to digital watermarking.

REFERENCES

[1] Sukriti Bhattacharya ,AgastinoCortesi,"*Data Authentication By Distortion Free Watermarking*", ICSOFT 2010.

[2] Jonathan Cummins, PatrickDiskin, Samuel and Robert parlett,"*Steganography and Digital Watermarking*" ,2004.

[3] Atul Kahate"*Cryptography and Network Security*".

[4] "Android Home Page"[Online].Available:http:/www.android.com

[5] "Android Developers"[Online].Available:http://developer.android.com/sdk/

[6] G.C. Langelaar, J.C.A van der Lubbe and J. Biemond,"*Copy Protection for multimedia data based on labeling techniques* ", 17th Symposium on Information Theory, 1996.

[7] Zhao Yuehua,"*An image watermark based onDiscrete cosine Transform block classifying*"

[8] Hye-Joo Lee, Ji-Hwyn Parkl and Yuliang Zheng2,"*Digital watermarking Robust Against JPEG Compression*".

[9] Chandra D V S 2002 Digital image watermarking using singular value decomposition. In: Proc. Of45th IEEE Midwest Symposium on Circuits and Systems Tulsa Oklahoma.

[10] G.C. Langelaar, I. Setyawan, and R. L. Lagendijk. "*Watermarking digital image and video data: A State-ofthe- Art Overview*," IEEE signal processing magazine. No.17, pp.20-46. September 2000.

[11] Clara Cruz Ramos, Rogelio Reyes, Mariko Nakano Miyatra-Keand Hector Manuel, "*Watermarking –Based Image Authentication System in the Discreet Wavelet Transform Domain*", Intechopen.

[12] http://blog.securemymind.com/wp-content/uploads/2012/11/encryption-awareness.png.