|| Volume 1 ||Issue 4 ||July 2016||ISSN (Online) 2456-0774
INTERNATIONAL JOURNAL OF ADVANCE SCIENTIFIC RESEARCH AND ENGINEERING TRENDS

COPYRIGHT PROTECTION FOR IMAGES ON MOBILE DEVICES

Ms. Roshni V. Misar

Student, Computer Science & Engineering, Everest College of Engineering & Technology, Aurangabad, India

Abstract:- **In this paper detailed description of LSB modification techniques and DCT based methods for watermarking is described. digital water marking generally used in as application in mobile handheld devices. So these two techniques as LSB and DCT are used to prevent from watermarking attack and energy consumption of the application done on android platform.**

Keywords- Digital water marking, DCT, LSB.

I INTRODUCTION

Now a day's cell phones (smart phone, tablet) rises their potential in terms of hardware and software. Mobile devices have operating systems such as android operating system and Symbian operating system. In past days, mobile plans were used for only sending message, playing video/audio, browsing etc. But now a day, smart phones are introducing with unbelievable changes such as image broadcasting etc.

Now, many of Smartphone apps presented in shops which segments the audio visual aid like pictures, videos etc. which can share pictures on social sites. This sharing process is done by taking images or by using image presenting services. But this images can easily downloadable by social networking sites or other sites and can easily uploaded. So, there is issue of copyright will arise. There is need to provide protection to images to avoid copyright problem and Prevent images from those people who do not have any rights to access it. This can be done using digital watermark, from this method we can embed the information into image.

This technique is typically used for finding the rights of the copyright of owner on water marked image, so we can define Water marking as hide digital information in an image data. This technique is used for validating the image authentication or to show the producer's identity. During this era mobile phones are used for many purposes such as browsing, sending and receiving emails, MMS services and many others.

II LITERATURE SURVEY

Data hiding is nothing but textual information can be covered behind graphical image in such a way that the unauthorized the user is unable to access. Data hiding processes following techniques are listed.

- Steganography
- Cryptography
- Digital signature

Stegnography: It means hiding the information behind the images which is nothing but encrypting is done by transmitter which the respected receiver only can decrypt and extract the information. Steganography. Yet such secure message stenography does not assurance to provide privacy to the statement. This problem is overcome by next technique.

Cryptography: The process of translating plain text into the cipher text is called as cryptography. Forgetting such translation two kind of keys a reused are public key and private key. Public key is used for encrypting and decrypting information and is recognized to every communicator over system. Every communicator has its individual private key and public key for security purpose which is used for decoding and encoding data[2].To improve cryptography another techniques are appeared.

Digital signature: It is a process of directing the message from one user to another in protected manner it means 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 attentive of sender public key. Digital signature strengths original verification and content integration services.[3]

Digital Water marking It is a technique that is used to insert hidden information into digital content, that data may be in the form of images ,videos, etc. If a digital case is affected by one or more logos, then the unknown information will be also carried in its replicas. One of the most important application of digital water marking is used as copyright protection. The digital water marking is used to prevent illegal copy of the digital media. There are mainly two types of digital water marking

- Invisible water marking
- Visible water marking

Visible water marking:

In this type of water marking image is covered by text in the form of watermark which is slight bit visible. And it is generally logos that is embedded over image [1][2]. Basically the main theme of visible water marking is that it alters

message which is watermark over a bitmap image then it combines text and image by picking the unsystematic pixels of the image [2]. That process of selection is totally reliant on the characters that are repeated in the watermarked string. Usually, visible watermarking offers one sort of certification to the image possessor because suppose if any other operator tries to remove the water marked string from image then the quality of the image is despoiled which reveals that the image is retrieved in an illegal manner. Thus in visible water marking image and the watermarked string are detectible to the user.

Invisible water marking:

Though the method of watermarking alteration is done in some part of multimedia information which is included in invisible watermarking. The watermarked text is not visual to the unapproved user. In this type Images are broken into number of blocks. These blocks involve of number of pixels. In invisible watermarking these pixels are transformed to embed the string over that image. By mutual image processing techniques the block that altered may be smashed. In this method content or the text is protected. In this category images is get protected nevertheless its representation is rejected by validation. Invisible watermarking is also used for image verification.[4].

III SYSTEM ARCHITECTURE OF PROPOSED SYSTEM

A. System Architecture :

Digital image processing is a speedily evolving zone with various raising applications in computer science and engineering .It is very significant field for the research work because its performances are used in almost all kinds of tasks like human computer boundary ,image enhancement, medical visualization; Law enforcement, image restoration and the most authenticated digital water marking for security purpose. Digital image processing has many beneficial belongings over the analogue image processing.

Digital image is used for various purposes like improving image quality, filtering images from noise and so on. A digital image [1] is made up of set of digital values as picture values which is called as pixels. Performing some operations on a digital image by using a digital computer is called digital image processing. The digital communication knowledge which may be turn into internet technology meets different problems which are related to the confidentiality and security of the information. Security techniques are vital because any one can access data without permission so that it is essential to protect information in the internet technology. In this paper we discusses about the digital water marking which provide encryption, decryption, cryptography, stenography and all. The digital water marking is an solicitation of the digital image processing.

Working :

Digital Water marking is a process which is used in the digital signal processing as inserting unseen information into program data. The programmatic information is not generally detectible, only devoted sensor or extractor can see and extracts this information. Digital Image Water marking use digital image for inserting the hidden information so that it is more secure which avoid external attack.

Below Figure1 shows the phases of digital water marking. Principally working of digital image water marking is distributed in three stages.

Embedding Stage:

It is the initial stage in which the logo is fixed in the original image by using the embedding algorithm and the secret key. Then the water marked image is created. So the water marked image is communicated over the network.

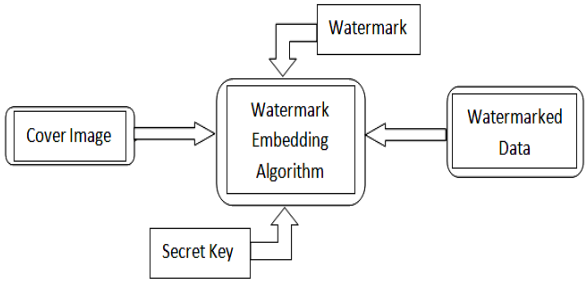


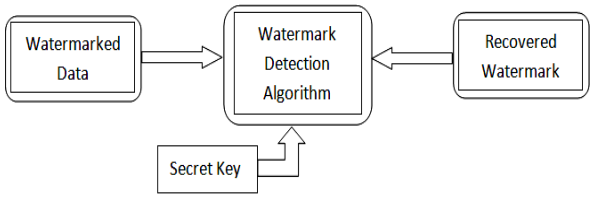
Figure1 : Water mark Embedding Process

Distortion/Attack Stage:

In this phase, when the data is transferred over the web. Also when some noise is added with the water marked image or some attacks are accomplished on the water marked image. So that water marked information is either modified or destroyed.

Extraction Stage:

In the detections stage the water mark is discovered or take out by the devoted sensor from the water marked image by put on some detection algorithm and by using private key. Also noise or distraction is also detected.



Figur2 : Water mark Detection Process

B. Algorithm Used:

Embedding algorithm :

The embedding algorithm takes two inputs i.e. cover image and watermark text.

START:

First step is to Check for length of watermark text.

(a) Convert watermark text into binary form let's consider it as X.

(b) Inverse that binary form.

(c) Check for condition.

If X is in odd form then algorithm will add 1 to X, and if it is in even form it will subtract 1 from X.

(d) Combine binary form with first LSB.

(e) Go to step 3 until finish.

(f) Save image.

END

The output image will be watermarked by text.

Extracting algorithm :

Extracting algorithm takes the watermarked image as input.

Start:

(a) At the first LSB of image get the length of text.

(b) Then Check for condition.

If X is odd then algorithm will add 1 to X, and if it is even it will subtract 1 from X.

(c) Get the binary form from LSB.

(d) Store it in array.

(e) Go to step 2 until finish.

(f) Convert binary array to character array

END

LSB Technique:

In LSB technique, the least significant bits of the cover image's digital data is use to cover up the message. The simplest way in LSB technique is replacement of the least significant bits. LSB replacement can flip the last bit of the data values to hide the message that needs for abstraction. Consider an 8-bit grey scale or color image where each pixel is store a byte value. [Checked] Suppose the first eight pixels of the original image have the following binary values:

10000000, 10100101, 10110100, 10110101, 11110010, 10110111, 11100110, 10110011

Now if we want to hide letter `Z' which have binary value as _1011010_. Following are the new values after replacing LSB of above pixels,

10000001, 10100100, 10110100, 10110101, 11110011, 10110110, 11100111, 10110010

IV MODULES USED

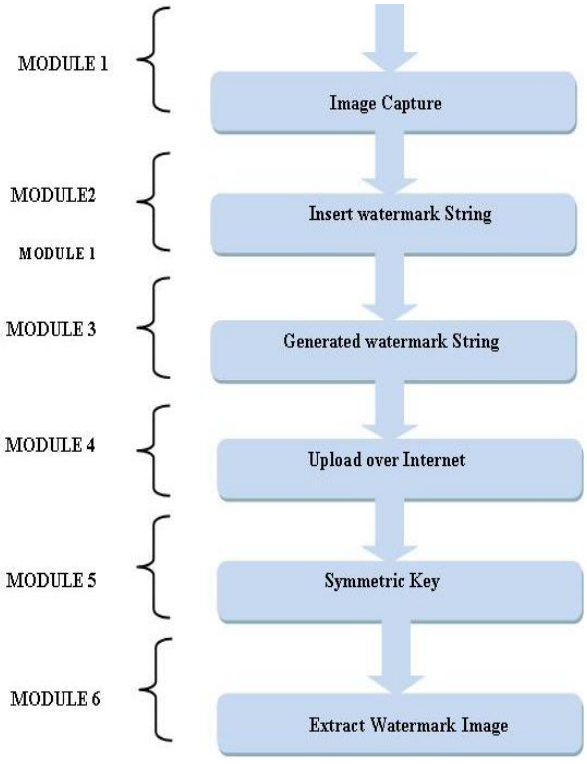


Figure3 : Modules Used

Modules :

This paper includes six components:

(a) Image Capture

(b) Insert watermark string

(c) Generated watermark

(d) Upload over internet

(e) Symmetric key

(f) Extract watermark

Module 1. Image Capture :

Take original image for inserting the watermark string and this technique is used to provide validation and user owner.

Module 2. Insert Watermark Message :

Embedding watermark string means encryption which is done on information and images by using the symmetric key. Encryption means converting text and images into code format.

Module 3. Generated Watermark :

After insertion of watermark string is become part of watermark images or data and is used for safe transferring the images or data over internet from illegal users.

Module 4. Uploaded Over Internet :

When watermark string is to be generated then it is easily able to upload over internet for allotment images and data with protected manner.

Module 5. Symmetric Key:

Symmetric key is key which is used for encryption and decryption purpose. For getting such transformation there are two types of keys are used which are nothing but public key and private key. Public key is used for encrypting and decrypting the data and is known to every correspondent over network. Every communicator has its own private key which is used for decrypting the encrypting data.

Module 6. Extract Watermark :

It is a technique to remove the embedded watermark string from original images and data and convert them from extracted images or data into original images.

V PERFORMANCE EVALUATION

A watermark is said to be a kind of information which is inserted into original data for interfere finding, localization, possession proof, and/or defector tracing purposes so watermarking methods apply to different types of cloud content. Digital watermarking is used to change that image in a such way so that we can see some script or circumstantial image without actually corrupting the image. In this way Watermarking is used to confirm the individuality and validity of the owner of a digital image. It is a process of verification of data which is inserted into digital image by owner. These signals be either video clip or pictures or audios. For example If Somebody attempts to copy the image, the watermark is copied along with the image.

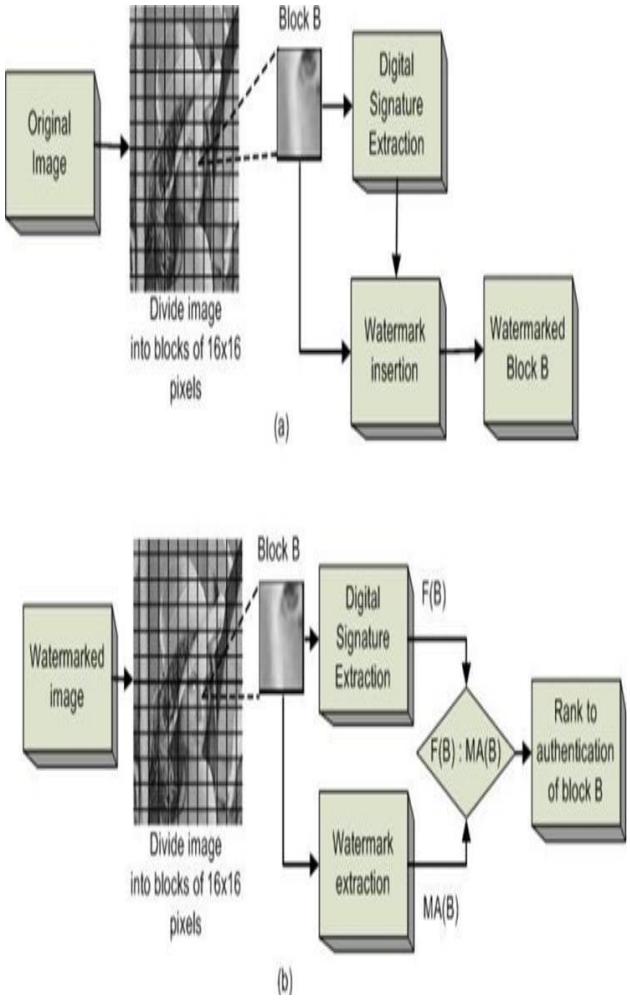


Figure 4: Watermarking Insertion And Extraction System.

VI CONCLUSION

Due to an evolution in the mobile devices in these eras prompts us to check on the security problems. There is necessity of giving the security to the user's multimedia assets and we can give that by water marking technique. We can also use this algorithm for android applications. The project gives the effective, reliable and secure method to prevent the images from mishandling. The images contain visible and invisible watermarks by which we can provide extra protection to the images So any tampering or editing done to the images can easily be detected. The original owner of the images can easily be found as the digital information is embedded on it. There are many techniques in data hiding.

The technique of Digital Watermarking is more protected and easy method of data hiding. All techniques of data hiding safe or protected data with their procedures but watermarking is extra proficient because of its proficiency. In Watermarking we mark the information which is to be hiding. The main goal of hiding information is security of data which is important today because of many reasons such as cyber-crime, which is highly improved day by day. Watermarking technique

gives us informal and competent security results of digital data. Watermarking provide security of not only images, but also audio video and text.

This section hopefully makes evident that watermarking as a technology is protected by copyright law. There is much scope for more research on the subject, and the dangers of missing the objective of reverse-engineering provisions in the Software Directive have been raised, and privacy concerns highlighted.

REFERENCES

[1] Raffaele Pizzolante, Bruno Carpentieri "Copyright Protection for Images on Mobile Devices"Dipartimento di InformaticaUniversitàdegliStudi di SalernoI-84084 Fisciano (SA), Italy raffaelepizz@hotmail.it, bc@dia.unisa.it978-0-7695-4684-1/12 $26.00 © 2012 IEEE DOI 10.1109/IMIS.2012.73

[2] Xia, C. Boncelet, and G. Arce, "A Multiresolution Watermark for Digital Images," Proc. IEEE Int. Conf. on Image Processing, Oct. 1997, vol. I, pp. 548-551.

[3] I. Cox, J. Kilian, F. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673-1687, Dec. 1997.

[4] M. Shensa, "The discrete wavelet transform: Wedding the a trous and mallat algorithms," IEEE Transactions on Signal Processing, vol. 40, no. 10, pp. 2464–2482, 1992.

[5] .Mitchell D. Swanson, Mei Kobayashi, Ahmed H. Tewfik, "Multimedia Data Embedding and Watermarking Technologies", Proceedings of the IEEE, 86(6):10641087, June 1998

[6] F. Bartolini, M. Barni, V. Cappellini, and A. Piva, "Mask Building for Perceptually Hiding Frequency Embedded Watermarks," Proc. Int. Conf. on Image Processing, Oct. 1998, vol. I, pp. 450-454.

[7] Yuan Y., Huang D., Liu D., "An Integer Wavelet Based Multiple Logo- watermarking Scheme", In IEEE, Vol-2, pp. 175-179, 2006.

[8] N. Ahmed, T. Natarajan, and K. Rao, "Discrete cosine transform," IEEE Transactions on Computers, vol. 100, no. 1, pp. 90–93, 1974.

[9] P. Bas, J. Chassery, and F. Davoine, "Using the Fractal Code to Watermark Images," Proc. IEEE Int. Conf. on Image Processing, vol. I, Oct. 1998, pp. 469-473.

[10] Reddy R., et al, "Robust Digital Watermarking of Color Images under Noise Attacks", International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009

[11] Wang Y., Doherty J.F., Dyck V.R.E., "A wavelet-based watermarking algorithm for ownership verification of digital images", IEEE Transactions, Image Processing, 11 pp. 77-88, 2002.

[12] Wang S.H., LinY.P., "Wavelet Tree quantization for copyright protection for watermarking", IEEE Transactions, Image Processing, pp. 154-165, 2002.

[13] Tao P., Eskicioglu A.M., "A robust multiple watermarking scheme in the discrete wavelet transform domain", Proceedings of the SPIE, Vol. 5601, pp. 133-144, 2004.

[14] Luo Y., et al. "Study on digital elevation mode data watermark via integer wavelets", Journal of software, 16(6), pp. 1096-1103, 2005.

[15] Lin Q., Lin Z., Feng G., "DWT based on watermarking algorithm and its implementing with DSP", IEEE Xplore, pp. 131-134, 2009.

[16] Chen, S.T., Huang, H.N., Chen, C.J., Wu, G.D., 'Energy-proportion based scheme for audio watermarking', IET Signal Process., 2010, 4,(5), pp. 576–587.