Android based digital watermarking using AES

Kiruthika.R[1], Monica.S[2], Kowsik.M[3], Manish Kumar.S[4], Sriram Ayyappan.R[5]
[1,2,3,4] *KGiSL Institute of technology*
Guided by
[5]*Assistant Professor, KGiSL Institute of Technology*

Abstract- **This paper deals with the effectuation of on demand, fast and user friendly android application, text and voice based system in digital watermarking. The purpose is to hide some information, like a copyright, into an image. With the increasing use of internet and effortless copying, tempering and distribution of digital data, copyright protection for multimedia data has become an important issue. The user can send the data through text or by voice. Human voice is converted into text by using android app and transmitted wirelessly through bluetooth to the processor 16F877 and then to the MATLAB software. The proposed method is block based scheme that uses the entropy and edge entropy as HVS characteristics for the selection of significant blocks to insert the watermark. The blocks of lowest entropy and edge entropy values are the best regions to insert the watermark. Singular Value Decomposition (SVD) is performed on the low-low sub-band to modify several elements in U matrix. This method shows high imperceptibility and high robustness against all image watermarking scheme. The security issue is improved by encrypting a portion of image by using Advanced Encryption Standard (AES). Finally the encrypted image is sent to the receiver. The receiver knows the decrypt key to split the secret data and image .The data is displayed on the LCD.**

Index Terms- **Android app, Block based DWT, HVS, SVD, AES.**

I. INTRODUCTION

Digital watermarking is derived from steganography. It is a technique which is supposed to embed some information into a media such as an image, video or audio document. This system focus on invisible watermarking and more precisely on images. Digital watermarking emerged as a tool for protecting the multimedia. In digital watermarking an imperceptible signal “mark” is embedded into the host image, which uniquely identifies the ownership. After embedding the watermark, there should be no perceptual degradation. These watermarks should not be removable by unauthorized person and should be robust against intentional and unintentional attacks. Digital watermarking is about constructing and analyzing protocols that prevent third parties or the public from reading private messages, various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography. It exists at the intersection of the disciplines of mathematics, computer science, electrical engineering, communication science and physics. Applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications. Here the information which has to be send is written by the user and it is sent through the android application to the MATLAB via Bluetooth module. There the image is split into four sub-bands low-low band, low-high band, high-high band, high-low band. The data is to be hidden in low-low sub-band with low sensitivity. The image with the data is encrypted providing a high level security to the information by Advanced Encryption Standard (Key 192 bits). Then it is sent to the receiver. At the receiver end, the receiver knows the secret key to decrypt the data. Finally the data is recovered from the image. This provides imperceptibility, robustness, noise, signal distortion and PSNR (Peak Signal to Noise Ratio) value is defined with mean squared error.

II.PROPOSED SYSTEM

The proposed scheme is a block based scheme, in which the secret data which is in the form of text or audio is send from the android application to bluetooth module. The secret data which is to inserted affects specific region of the image. DWT is applied to each selected block individually. The advantage of using this block is less computational time compared to other techniques. The image is split into four sub-bands they are low-low band, low-high band, high-high band, high-low band. An SVD is performed on the transformed coefficients of the LL sub-band of each block. Embedding in SVD vectors will improve the robustness, invisibility and security. The number of pixels of an image at different intensities are shifted in histogram shifting. Several of the required secret keys are encrypted using Advanced Encryption Standard. Then it is sent to the receiver. At the receiver end, the receiver knows the secret key to decrypt the data. Finally the data is recovered from the image.

III.HARDWARE SPECIFICATION

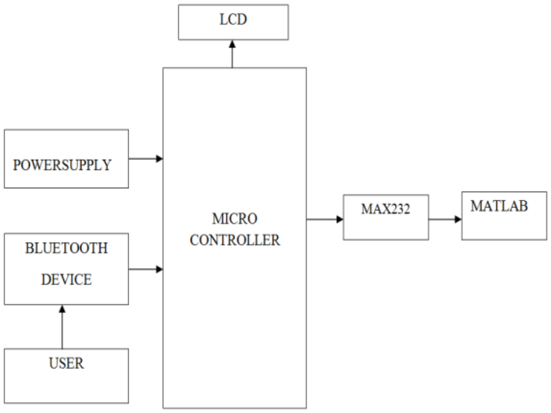

Fig1.Block diagram

IV.COMPONENTS

POWER SUPPLY

The ac voltage, typically 220V rms, is connected to a transformer, which steps that ac voltage down to the level of the desired dc output. A diode rectifier then provides a full-wave rectified voltage that is initially filtered by a simple capacitor filter to produce a dc voltage. This resulting dc voltage usually has some ripple or ac voltage variation. A regulator circuit removes the ripples and also remains the same dc value even if the input dc voltage varies. This voltage regulation is usually obtained using one of the popular voltage regulator IC units.

LIQUID-CRYSTAL DISPLAY

LCDs are available to display arbitrary images (as in a general-purpose computer display) or fixed images with low information content, which can be displayed or hidden, such as preset words, digits, and 7-segment displays as in a digital clock. They use the same basic technology, except that arbitrary images are made up of a large number of small pixels, while other displays have larger elements. LCD is used to display the secret data on the receiver side.

MAX232

In communications, RS-232 is a standard for serial binary data interconnection between a DTE (Data terminal equipment) and a DCE (Data Circuit-terminating Equipment). It is commonly used in computer serial ports.

In this circuit the MAX 232 IC used as level logic converter. The MAX232 is a dual driver/receiver that includes a capacitive voltage generator to supply EIA 232 voltage levels from a single 5V supply. Each receiver converts EIA-232 to 5V TTL/CMOS levels. Each driver converts TLL/CMOS input levels into EIA-232 levels. In this circuit the microcontroller transmitter pin is connected in the MAX232 T2IN pin which converts input 5V TTL/CMOS level to RS232 level.

In PC the transmitting data is given to R2IN of MAX232 through transmitting pin of 9 pin D type connector which converts the RS232 level to 5V TTL/CMOS level. The R2OUT pin is connected to receiver pin of the microcontroller. Likewise, the data is transmitted and received between the microcontroller and PC or other device vice versa.

BLUETOOTH MODULE

The Bluetooth module HC-05 is a MASTER/SLAVE module. By default the factory setting is SLAVE. The Role of the module (Master or Slave) can be configured only by AT COMMANDS. The slave modules cannot initiate a connection to another Bluetooth device, but can accept connections. Master module can initiate a connection to other devices. The user can use it simply for a serial port replacement to establish connection between transmitter and receiver.

PIC16F877A

This powerful (200 nanosecond instruction execution) yet easy-to-program (only 35 single word instructions) CMOS FLASH-based 8-bit microcontroller packs Microchip's powerful PIC® architecture into an 40- or 44-pin package and is upwards compatible with the PIC16C5X, PIC12CXXX and PIC16C7X devices. PIC16F877A features 256 bytes of EEPROM data memory, selfprogramming, an ICD, 8 channels of 10-bit Analog-to-Digital (A/D) converter, 2 additional timers, 2 capture/compare/PWM functions, the synchronous serial port can be configured as either 3-wire Serial Peripheral Interface (SPI™) or the 2-wire Inter-Integrated Circuit (I²C™) bus and a Universal Asynchronous Receiver Transmitter (USART). All of these features make it ideal for more advanced level A/D applications in automotive, industrial, appliances and consumer applications. This is used for controlling module in embedding the image.

V.SOFTWARE SPECIFICATION

BLOCK BASED DISCRETE WAVELET TRANSFORM

Block based DWT is the ability to process each block individually. It can able to embed the watermark into the selected blocks, which are the blocks or regions bearing the basic character information of the image, such as the texture and edges. This tool provides multiple-resolution analysis of an image. The image decomposes into two components :high frequency and low frequency. The decomposition process is done by passing the signal through a series of high-pass filters to analyse the high frequencies and passing the signal through a series of low pass filters to analyse the low frequencies. Moreover, signals are analyzed at different resolutions by using filters with different cut-off frequencies. The frequency components are further divided into four sub-bands (LL,HL,LH and HH). The secret text is inserted in the low-low sub-band. Embedding the watermark in the low frequency provides greater robustness, imperceptibility and less sensitive to change.

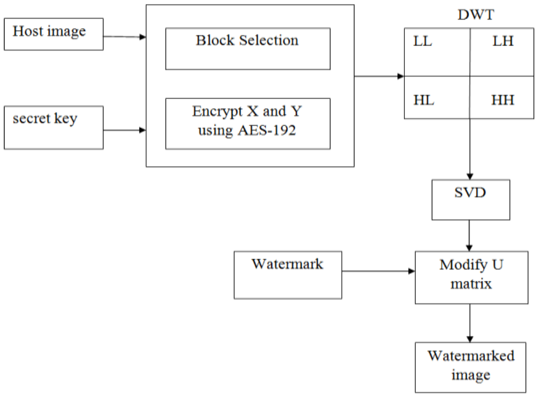

Fig2.Embedding process

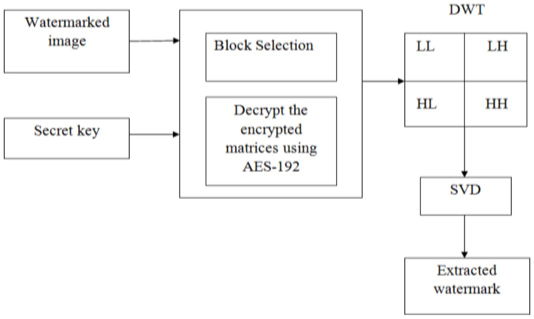

Fig3.Extraction process

SINGULAR VALUE DECOMPOSITION

SVD is commonly used to maintain the good stability and applying an SVD to an image does not noticeably affect the appearance when a small interfering signal is added to the image. It is applicable to noise reduction, image compression and image watermarking.

HUMAN VISUAL SYSTEM

HVS characteristics are employed to select the desired blocks by calculating the entropy and edge entropy for each block. These two obtained values are summed, and resulting magnitude values are sorted in ascending order. It is desired to modify the minimum number of edge points of the host image during the embedding process.

ADVANCED ENCRYPTION STANDARD

The AES has three fixed 128-bit block ciphers with cryptographic key sizes of 128,192 and 256 bits. Key size is unlimited whereas the block size maximum is 256 bits. Features of AES are block encryption implementation,128-bit group encryption with 128,192 and 256-bit key lengths, symmetric algorithm requiring only one encryption and decryption key, data security for 20-30 years, world wide access, no royalties, overall implementation.

PEAK SIGNAL-TO-NOISE RATIO

PSNR is defined as a ratio between the maximum possible power of a signal and the power of corrupting noise. It is most commonly used to measure the quality of reconstruction of lossy compression codecs. the signal in this case is the original data, and the noise is the error introduced by compression. When comparing compression codecs, PSNR is an approximation to human perception of deconstruction quality. Typical values for the PSNR in lossy image and video compression are between 30 and 50 dB.

MEAN SQUARED ERROR

PSNR is often described as MSE it measures the average of the squares of the errors or deviations - that is, the difference between the estimator and what is estimated. It is the measure of the quality of an estimator -it is always non- negative and values closer to zero are better.

VI.CONCLUSION

In this paper, a DWT-SVD block based image watermarking scheme is presented in which several characteristics were employed to achieve high level grades for the watermarking requirements and maintain the tradeoff between them. The HVS characteristics of entropy and edge entropy were used to select the low informative blocks as the best embedding region. This it provides high robustness on maintaining non noticeable distortions, that is to maintain imperceptibility. In terms of robustness good resiliency was observed against all types of image processing attacks and several types of geometrical attacks. This it is mainly used in the application field of defense, medical and e-government

REFERENCES

[1] Ahmed S. Salama, Mohamed Amr Mokhtar ,"Combined Technique For Improving Digital Image Watermarking" , published in: computer and communication (iccc), 2016 2nd ieee international conference on 14-17 Oct 2016, INSPEC Accession Number:16867710, IEEE.

[2] Ali Al-Haj, Hussam Barouqa, "Copyright Protection Of E-Government Document Images", Information Management (ICIM), 2017 3rd International Conference on 21- 23 April 2017, INSPEC Accession Number: 16967192, IEEE.

[3] Oswaldo Juarez-Sandoval, Eduardo Fragoso-Navarro, Mariko Nakano, "Improved Unseen-Visible Watermarking For Copyright Protection Of Digital Image", Biometrics and Forensics (IWBF), 2017 5th International Workshop on 4-5 April 2017, INSPEC Accession Number: 16917434, IEEE.

[4] Tao Wang, "Digital Image Watermarking Using Dual-Scrambling And Singular Value Decomposition", Computational Science and Engineering (CSE) and Embedded and Ubiquitous Computing (EUC), 2017 IEEE International conference on 21-24 July 2017, INSPEC Accession Number: 17098789, IEEE.

[5] Sudhanshu Suhas Ginge, Vilas M. Thakare, Ashok A. Ghatol, Siddharth A. Ladhake, "Combined DWT Image Watermarking and AES Technique for Digital 2-D Image", Recent Advances and Innovations in Engineering (ICRAIE), 2016 International Conference on 08 June 2017, INSPEC Accession Number: 16933042, ISSN :5090-2806, IEEE.

[6] S. Ponnisathya, S. Ramakrishnan, S. Dhinakaran, P. Sabari Ashwanth, P. Dhamodharan, "CHAOTIC map based video watermarking using DWT and SVD", Inventive Communication and Computational Technologies (ICICCT), 2017 International Conference on 10-11 March 2017, INSPEC Accession Number: 17042278, IEEE.

[7] Ritu Gupta, Pulkit Mundra, Shikha Karwal, Abhilasha Singh, "DWT-SVD Based Watermarking Scheme of JPEG Images Using Elliptic Curve Cryptography", Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 2016 5th International Conference on 7-9 Sept 2016, INSPEC Accession Number: 16544226, IEEE.

[8] Rijia M Raju, K.Gopakumar, "An image authentication technique based on cross chaotic map", Computational Systems and Communications (ICCSC), 2014 First International Conference on 17-18 Dec 2014, INSPEC Accession Number: 14931670, IEEE .

[9] Fathima Nasreen K, P. Chitra, "A robust encryption and digital watermarking scheme for dicom images using quaternion's and dwt-svd", Green Engineering and Technologies (IC-GET), 2016 Online International Conference on 19 Nov 2016, INSPEC Accession Number: 16864584, IEEE.

[10] Jasdip Kaur, Narwant Singh, Chahat Jain, "An Improved Image Watermarking Technique Implementing 2-DWT and SVD", Recent Trends in electronics, Information & Communication Technology (RTEICT), IEEE International Conference on 20-21 May 2016, INSPEC Accession Number: 16583127, IEEE.