Hybrid Steganography Toolkit for Mobile with Air Signature Security

Nishu Kumari, Anuja Kamble

***Abstract*— Improving the security of applications is one of the crucial points required to assure the personal information .This paper presents a biometric authentication procedure consisting of verifying the identity of valid users by making a signature in the air while holding the mobile phone. The verification of the identity will open up the application of steganography which consist of image on which various processing techniques can be applied. This model is based on messy watermarking scheme for the authentication of images.First it separates RGB colors of a pixel of image, dynamically generates the watermark using messy models by applying Chaos algorithm and it is embedded inside the image by expanding intra plane difference between any two color planes of images known as intra plane difference expanding. All the above process comes under primary watermarking. Then alpha channel embedding algorithm is used in next step for secondary watermarking. The final image generated is sent over a network and this Authentication guesses whether that received image has been modified or not and detect the tempered regions.**

***Index Terms*— Steganography,In-Air Signature,RGB Color Seaperation,Digital Wtarmarking,Alpha Channel Embedding.**

I. INTRODUCTION

When the private images are exchanged in public or private network, major issue is related to authentication of an image. This checks that image received by receiver is received without getting modified in between its path and is received by the proper source. This security can be explained in two terms 'copy right protection' and 'authentication'. Copy right protection is an effort designed to prevent the reproduction of media, for copyright reasons. Authentication guesses whether that received image has been modified or not and detect the tempered regions. The requirements for these two applications of watermarking are different. Embedded watermark should be robust to attacks in copyright protection. And the watermark should be fragile to the attacks in authentication. So that receiver can easily break that watermark for authentication purpose. Sensitiveness of the watermarking can be given in terms of frailty.

Mobile phones plays a vital role where people may perform a lot of operations such as e-commerce applications. In addition to this, mobile phones store a lot of personal information that should not be revealed to anyone except the owner of the phone. Therefore, mobile phones are nowadays very useful devices, but they require security in order to keep safe the information and the operations performed with them. In this context, biometrics could help complementing or substituting PIN-code security. There are many works including biometric authentication techniques in mobile devices to enhance their security.

This technique is based on authenticating people by making their signature in the air while holding their mobile phone in their hand. This biometric technique has similarities with handwritten signature.

Manuscript received February 01, 2015.

Nishu Kumari, Computer Science, Bharati Vidyapeeth College of Engineering for Womens, Pune,India.

Anuja Kamble, Computer Science, Bharati Vidyapeeth College of Engineering for Womens, Pune,India.

II. PROPOSED SYSTEM

The proposed watermarking scheme in this paper works in four stages. The first stage selects the reference color plane for generating watermark. The second stage generates the watermark using the reference color plane through messy system. The Embedding process is carried out using integer transformation in third stage.The forth stage performs the extaraction and verification process.

A. FIRST STAGE: Air Signature Authentication

In this stage Air signature, user will make signature in air for authorization purpose[1]. First three to four attempts of signature of one person will be taken and will get stored in database. The user will make signature in air same as made before and we will check both of the signatures with Euclidian algorithm[3-4] by comparing its x, y, z coordinates values. If both signature matches then steganography application will get open.

B. SECOND STAGE: RGB Separation

Image Pixels are stored as integers. The integer can be 8-bit,24-bit or 32-bit depending on image type,most popular are 24-bit color image where 8-bits each for Red, Green And Blue color values[9] are used to Represent a 24-bit pixel values.

Sample PIXEL values in HEX=0EDEB5
• Then individual color channels:

Here we have taken red,green and Blue values for comparision purpose and shifting the bits by 8bit,16 bit to get the colors separated.

• In programming the hex numbers are represented as 0x0EDEB5. 0x prefix is for hex notation.
• 0E (red) - DE (green)- B5 (blue)
• 00001110 – 11011110 – 10110101
• Actual Color Composed Will Be :
Traverse Through Entire Image.

```
for(x=0;x<width;x++)
{pix=input[y][x];
Extract 8-bit R,G and B values from 24-bit Color Value
b=pix &0xff;
g=(pix>>8)& 0xff;
}
```

For Green we shall first right shift the pixel value by 8 bits so that green component is now at LSB position. And then repeat the masking process.

Eg: 435A56 >> 8 = 435A

0x435A

AND 0x00FF

0x005A-green separated

Similarly we shall right shift by 16 bits so that red component will be at the LSB position and then do the masking.

C. THIRD STAGE : Watermark Generating

In this paper for watermark generation of Messy model we are applying Chaos Algorithm[5]. The behaviour of messy model is dynamic and changes with time. The watermark is generated using the reference color plane as initial condition. This theory creates a planned randomness[7] using a particular equation. Finally, the digital watermark[6] is generated firmly.

Messy system is a system whose behavior changes firmly with time[2]. These changes are extremely sensitive to the initial conditions. This sensitivity manifests changes exponentially with the initial conditions.

Thus, the behavior of messy system appears to be random, though they are deterministic. The dynamic changes of this system are completely defined by their initial conditions without any random elements. A general messy system is defined by the following equation

$$x_{n+1} = f(x_n)$$

Where f(*) refers the iterative, non linear function. It iteratively produces the values for initial value. It is known as messy sequence. The iteration will be stopped, when the parameters in f(*) satisfy a certain requirements for messy status. Once the sequence reached the messy status, it can be used to generate the watermark. In the proposed system, a hybrid optical bi stable messy system [23] is used which is defined by

$$f(x_n) = 4\cos^2(x_n - 3.5)$$

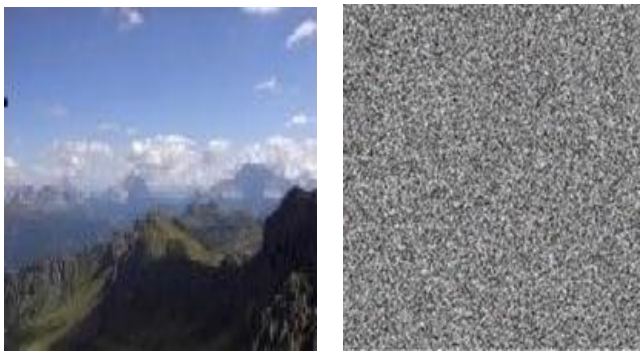
The watermark is generated through messy system[8] by using prominent pixel values of reference color plane of the image as seed. The initial values to the messy system is designed by

$$c\_seq(k,0) = a * floor(s(k)/2^l) * 2^l + b * pos + c * key$$

Where, s(k) refers the pixel values of reference color plane of the image. a, b and c are predefined constants and I refers embedding depth. The position information (pas) and secret key (key) is also used in the initial condition. The messy sequence is generated by substituting c_seg (k, 0) value for Xn in Eqn.2.For the kth pixel the sequence is referred as c_seq (k, i), i=l, 2, 3 ... 1 The reasonable number of iteration (I) is performed for the □ pixel to attain the messy status. This sequence contains floating numbers that is converted in to binary sequence in the proposed scheme. Hence, the thresholding T is introduced here to convert the sequence c_seq (k, i) from floating to binary sequence w (k, i). The w (k, i) is obtained by

$$w(k,i) = \begin{cases} 1 & c\_seq(k,i) > T \\ 0 & Elsewhere \end{cases}$$

Where, T is set to 8/3 by the number of test to bring equal number of zeros and ones [24]. The length of sequence G is combined to one bit w (.) by applying XOR operation. Thus, the watermark is generated for the kth pixel. By repeating the same procedure for remaining pixels of the reference color plane of the image, the watermark is generated for the whole image.



A B

Fig 3. A) Main image, B)Generated watermark

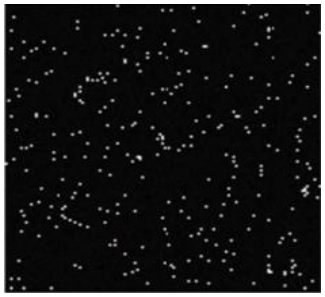
D. FOURTH STAGE: Watermark Embedding

In this stage the generated watermark will be embedded by using intra-plane difference expanding. In difference expansion we expand the difference between any two pixels by keeping their average constant. Any color plane can be used as root to generate the watermark . The watermark is unique to the images as it is generated firmly. Then, pixel pair is formed from the remaining two color planes of the images.

The watermark is embedded, by checking overflow and underflow condition for pixel pair [8]. This is known as intra-plane
difference expanding.

A B

C



D E

Fig 4. A) Main image, B) Generated watermark, C)Watermarked image, D) Tmepored image, E)Error image

E. FIFTH STAGE: Extraction and Alpha channel embedding

In this stage of extraction, the watermarked image (WM image) is processed and the reference sequence is produced using messy system and reference color plane as seed. The embedded watermark is extracted by applying inverse integer transform. Where, the LSB (Least Significant Bit) of the difference value gives the embedded watermark bit. The reference sequence and the extracted watermark sequence are compared to check that whether the given volume of the image is tampered or not. The difference between reference sequence and the extracted watermark sequence will show the tampered volumes in the image. Thus, extraction process enhances the security. The extraction process in this paper is reversible. It means that the original image should be retrieved without any loss after removing the watermark at the extraction stage. The loss in the quality of images is not accepted here[10][11][12-29]. After the extraction process here comes the verification in which we are using Alpha channel embedding to authenticate our image. With this we are providing transparency to it. A few of the image formats provide support for this which represents up to 256 levels of transparency . With this technique the image can be ported to other applications while retaining transparency.

III. CONCLUSION

In this paper, we present a biometric authentication procedure consisting of verifying the identity of valid users by making a signature in the air while holding the mobile phone embedded with accelerometer verification of the signature opens up the steganography application in which a messy watermarking scheme has been proposed for image authentication. RGB separation separates red, green and blue color of each pixel of an image. Chaos algorithm creates planed randomness in main image and generates the watermark dynamically using messy models. Generated watermark is then embedded in the main image by expanding the difference of the pixel pair formed in intra color plane. If any region of image is tempered then it could be located. Watermark extraction process does not depend on the knowledge of both original and watermarked image.

ACKNOWLEDGEMENTS

First and foremost we would like to express our gratitude to Prof. D.D Pukale, our internal guide and HOD , for his guidance and support throughout the project. Without his cooperation, it would have been extremely difficult for us to complete the project part of this semester. . We would like to thank the entire teaching and non-teaching staff of the Computer Department for giving us an opportunity to work on such an exciting project. Last but not the least, we are extremely grateful to our family, friends and colleagues who have supported us right from the inception of the project. Thanks for all your encouragement and support.

REFERENCES

[1].Time series distances measures to analyze in-air signatures to authenticate users on mobile phones
Javier Guerra-Casanova, Carmen Sa´nchez A´ vila, Gonzalo Bailador, Alberto de-Santos-Sierra
Centro de Dom´otica Integral Universidad Polit´ecnica de Madrid Campus de Montegancedo 28223 Pozuelo de Alarc´on, Madrid, SPAIN
Email:[jguerra, csa, gbailador, alberto]@cedint.upm.es

[2]. Review on Surround Sense Hand Gestures for Mobile Devices
Pravin Raut ME 3rd sem WCC, PCE RTM Nagpur University Nagpur, India, Snehal Golait Dept. CT, PCE RTM Nagpur University Nagpur, India.

[3]. "Cluster analysis". March2,2011.

[4]. Deza, Elena; Deza, Michel Marie(2009)Encyclopedia of distances. Springer. P. 94.

[5]. Applied Mathematical Sciences, Vol. 8, 2014, no. 32, 1593 – 1604
HIKARI Ltd, 2 Robust Chaos Based Image Watermarking Scheme for Fractal-Wavelet P. Shanthi**,** Anna University, Chennai, India.R. S. Bhuvaneswaran**,** Anna University,Chennai,India

[6]. Safeguarding the Digital Contents: Digital Watermarking M. Natarajan and Gayas Makhdumi1 NISCAIR, 14, Satsang Vihar Marg, New Delhi-110 067
E-mail: m_natarajan@hotmail.com
1Department of Library & Information Science, Jamia Millia Islamia University, New Delhi-110 025.E-mail: gayas_makhdumi@yahoo.co.in

[7]. A New Steganographic Method Based on Information Sharing via PNG Images Che-Wei Lee Institute of Multimedia Engineering National Chiao Tung University, Hsinchu,Taiwan.

[8]. Lossless fragile pinpoint authentication scheme for medical images Poonkuntran,S.Dept. of Technol., Velammal Coll. Of Eng. & Tecnol., Madurai, India ; Rajesh, R.S.

[9].ADynamic Watermarking Model For Medical Image Authentication,Priya H & anitha.1,2Dept. of ECE, EWIT, Bangalore, India.

[10]. G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, R. Collorec, "Relevanc of Watermarking in Medical Imaging", in Information Technology Applications in Biomedicine, IEEE-EMBS Conference, Arlington, USA, pp. 250-255, Nov. 2000.

[11]. N. Zhicheng, Y.Q. Shi, N. Ansari, S. Wei,"Reversible data hiding", in proc. ISCAS '03, Circuits and Systems, International Symposium on, May 2003, Vol. 2, pp. 25-28.

[12]. S. Waiton, "Image authentication for a slippery new age", Dr. Dobb's 1. 20 (1995) 18-26.

[13]. M. Yeung, Mintzer, "Invisible watermarking for image verification", 1.Electron. Imag. 7 (1998) 578-591.

[14]. M.Wu, B. Liu,"Watermarking for image authentication", in: Proceedings of the IEEE International Conference on Image Processing, Chicago, IIIinoise,US, (1998), pp. 437-441.
[15].M.Holliman,N.Memon, "Counterfeiting attacks on oblivious blockwise independent invisible watermarking schemes", IEEE Trans. Image Process. 9 (2000) 432-441.
[16]. M.U. Celik, G. Sharma, E. Saber, AM. Tekalp, "Hierarchical watermarking for secure image authentication with localization", IEEE Trans. Image Process. 11 (2002) 585-595.
[17]. M. Celik, G. Sharma, A Tekalp, "Lossless watermarking for image authentication: a new framework and an implementation", IEEE Trans.Image Process. 15 (2006) 1042-1049.
[18] 1.Wu, B. Zhu, S. Li, F. Lin, "A secure image authentication algorithm with pixel-level tamper", in: International Conference on Image Processing, Singapore, October, (2004), pp. 1573-1576.
[19]. 1. Fridrich, "Image watermarking for tamper detection", in: IEEE Inter.Conf. on Image Processing, Chicago, Illinois, USA, (1998), pp. 404-408.
[20]. Rongrong Ni , Qiuqi Ruan, Yao Zhao, "Pinpoint authentication watermarking based on a chaotic system", Forensic Science International Journal,VoI.No: 179,Page.No: 54-62,2008.
[21]. D.-C. Lou, et aI., "Multiple layer data hiding scheme for medical images", Computer Standards & Interfaces (2008), doi: 10.1016/j.csi.2008.05.009
[22]. 1. Tian, "Wavelet-based reversible watermarking for authentication", Proceedings of SPIE on Security and Watermarking of Multimedia Contents IV, vol. 4675, Jan.2002, pp. 679-690.
[23]. T.-S. Chen, C.-C. Chang, M.-S. Hwang, "Virtual image cryptosystem based upon vector quantization", IEEE Transactions on Image Processing 7(10)(Oct 1998)
[24]. 1. Fridrich, M. Goljan, R. Du, "Lossless data embedding –new paradigm in digital watermarking", EURASIP Journal of Applied Signal Processing 2002 (2)(Feb.2002) 185-19
[25]. 1. Tian, "Reversible data embedding using a difference expansion", IEEE Transactions on Circuits and Systems for Video Technology 13 (8) (Aug. 2003) 890-893.
[26]. 1. Tian, "Reversible watermarking by difference expansion", Proceedings of Workshop on Multimedia and security : Authentication, Secrecy, and Steganalysis, Dec. 2002, pp. 19-22.Workshop on Multimedia and Security: Authentication, 22.
[27]. 1.M. Barton, "Method and Apparatus for Embedding Authentication InformationWithin Digital Data," U.S. Patent 5, pp. 646-997,1997.
[28]. H. Fujita, et aI., Computer-aided diagnosis: "The emerging of three CAD systems induced by Japanese health care needs", Computer Methods and Programs for Biomedicine.(2008).
[29]. Nammer N, EL-Emman, "Hiding a Large Amount of Data with High Security using Stegnography Algorithm", Journal ofComputer science, vol 3,Issue 4,PageNo 223-232,2007.