I J C T A, 9(37) 2016, pp. 999-1008

Turing Machine Verification Security System

A. Maheshwari[*] and M.A. Dorai Rangaswamy[**]

Abstract: **T**he effort recommends to identify the biometric safety system created on variation of palm print and graphical image by steganography technique designed for Validation resolution. Here the secret pin facts hiding method using Turing Machine involve disguise anonymous individual information in the interior of their biometric to enhance the privacy protection. The graphical images such as some common images are used for account verification purpose. The palm print appearance is related and collected conferring to the key opinions. The landscapes of the tribute print remain extracted using Weber's Local Descriptor. The structures of palm pattern besides graphical image are then associated through stored folder grade copy nose courses then it's approved by means of Euclidean or Hamming distance. Uncertainty this element is ended effectively before handler material which comprises being confirmation amount through four numerals main resolve remain coordinated through take out facts since now unseen copy aimed at additional equal safety. Lastly the multimodal scheme lengthways by means of steganographic technique displays the greatest course correctness aimed at this involuntary identification and verification application.

Index Terms: Cryptography, Multimodal biometrics, Bits wrap, WLD, Chaos encryption, LWT, JFLAP, CFG.

1. INTRODUCTION

Multimodal biometric schemes custom Numerous devices or biometrics to overwhelmed the confines of unimodal biometric schemes. Though unimodal biometric organizations remain incomplete by the quantity of biometrics used there. Multimodal biometric structures container encompass a groups of material since dissimilar biometrics. Multimodal biometric organisms dismiss participate these unimodal methods and perform operations over that. User verification system that uses unimodal biometric indicator often has to overcome erroneous data. Instead multimodal biometrics helps to achieve an increase in performance [1].

In this work it involves three steps of operation. They are database creation, testing and recognition mode. In database creation step, the samples of palm print and graphical images are obtained from user. The obtained samples be present put away in the catalog. In the testing mode, the samples are tested whether it belongs to the correct user. In the recognition mode, the features that are removed since the tasters stored in the database are matched with the landscapes haul out beginning the illustrations the user has chosen for their recognition. For recognition mode, features form the core for processing and their extraction plays an important role in the recognition [2].

In this work, palm print and graphical images are taken. Graphical images are some common images that the user can remember easily. Here before the enrollment of the user, the admin has to click on the one time click image so as to enter for the user enrollment. Since the image is to be clicked only once at a time, it will be more secure than other systems. The key goal of this procedure remains to reduce the error rate and improve security.

Steganography [3] be situated the concert of allocation material in an unrecognizable way that nobody can predict the incidence of the data. Cryptography and Steganography techniques are used to prevent attacks from unauthorized users [3]. Weber's Local Descriptor is used to describe texture features of images

[*] Research Scholar, Sathyabama University, Chennai. *Email: 78mahee@gmail.com*
[**] Professor, Department of CSE, AVIT, Chennai. *Email: drdorairs@yahoo.co.in*

which contain two components. The first component is difference excitation plus it computes power of the recent pixel. The second module is the incline location and it computes the qualified strength variances [4].

2. PROPOSED SYSTEM

The proposed system contains three phases: Enrollment of user, Verification and Testing. Before the enrollment, the admin has to click on the one time click image to enter for the enrollment of the user. The image has a specific point which has to be clicked only once. If the point is wrongly clicked, then the user cannot enter for enrollment. This is a main security in this paper. Figure 1 shows the overall system architecture.

2.1. Data Base Creation

The palm print and the graphical image are obtained from the user. The obtained palm print is a color image and so the planes of the palm print are separated. The blue plane is taken because the hiding capacity then the duplicate inferiority of the blue plane are high. The palm print is cropped using the cropping command in MATLAB. And the cropped palm print is stored in the data base. The graphical image is any of the user defined image. The features of the graphical image are extracted. The features are extracted in order to match the features during the recognition phase. The palm print and the graphical image that are chosen by the user are stored in the data base.

The geographies are take out using Weber's Limited Descriptors. Conferring to this decree the share of the raise beginning and the amount is persistent. WLD descriptor is used for texture representation. The control of WLD descriptor comprises three stages i.e. discovery discrepancy excitations, incline locations and construction the histogram. The Weber's law can be denoted as,

$$\frac{\Delta \mathrm{I}}{\mathrm{I}} = k \tag{1}$$

where, ΔI is the increment threshold and I is the original intensity and k is the constant.

2.1.1. Discrepancy Excitation

It uses the strength variances amid its nationals and a existing pixel as the fluctuations of the existing pixel. It could be explained using the following matrices.

V_s^{11}	V_s^{12}	V_s^{13}
V_s^{21}	V_s^{22}	V_s^{23}
V_s^{31}	V_s^{32}	V_s^{33}

Principal compute the alterations among its nationals and the epicenter idea from the above matrix,

$$\mathrm{V}_s^{11} = \sum_{i=0}^{p-1} (\Delta x_i) = \sum_{i=0}^{p-1} (x_i - x_c) \tag{2}$$

where ($i = 0, 1, \ldots p - 1$) signifies the i-th fellow citizen of x_c and p is the quantity of foreigners. We before Figure the relation of the alterations to the power of the existing opinion by uniting the productions of the binary riddles. The discrepancy excitation of the existing pixel $\xi(x_c)$ is figured as:

$$\varepsilon(x_c) = \arctan\left[\frac{\mathrm{V}_s^{11}}{\mathrm{V}_s^{12}}\right] = \arctan\left[\sum_{i=0}^{p-1}\left(\frac{x_i - x_c}{x_c}\right)\right] \tag{3}$$

$\xi(x)$ might gross a detriment price if the national forces are slighter than that of the recent pixel. If $\xi(x)$ is helpful, it signposts that the settings are sunnier than the up-to-date pixel. In disparity, if $\xi(x)$ is adverse, it indicates that the environs are shadier than the existing pixel.

2.1.2. Slope Direction

Succeeding foremost section of WLD is ramp orientation. For a pixel the slope orientation is considered as surveys

$$\theta(x_c) = \arctan\left[\frac{V_s^{22}}{V_s^{21}}\right] \tag{4}$$

Where v_s^{22} is the passion modification of two pixels on the absent and correct of the contemporary pixel x_c, and v_s^{21} is the amount alteration of dualistic pixels right below and upstairs the present-day pixel.

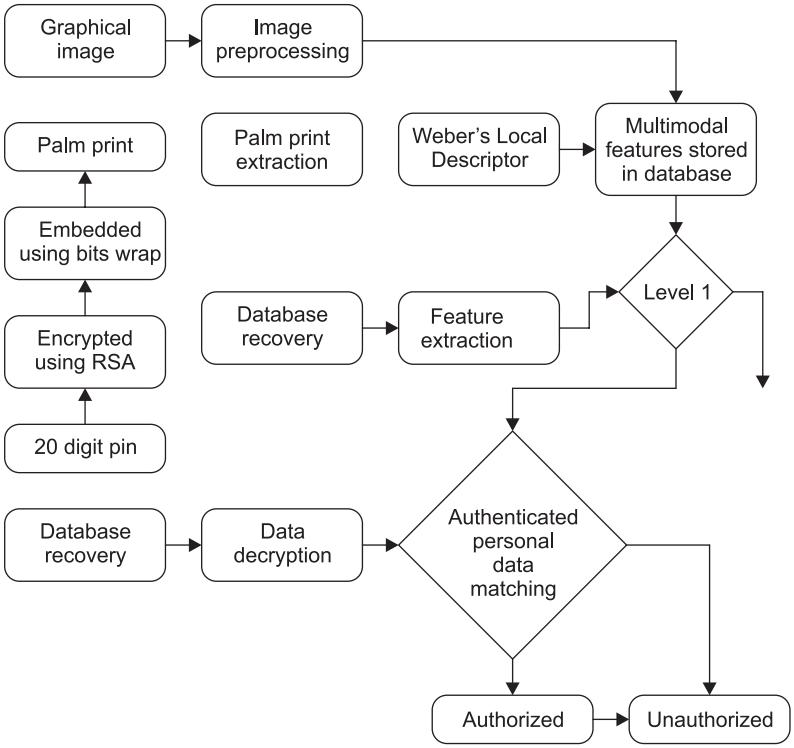

Figure 1: Overall System Architecture

2.2. Data Encryption and Data Hiding

A 4 digit pin is obtained from the user. The 4 digit pin is combined with that of the 16 digit pin that is stored defaultly. The 16 digit pin varies for different user.

The 20 digit pin is encrypted using TM. For all encryption 20 states is used. For all state the given number is translated into the next number. Turing Appliance as a mechanism through a determinate amount of switch conditions and an immeasurable adhesive tape, restricted at the leftward and extending off to the true. The friction tape is separated into lockups, both of which can grip one representation. The involvement of the engine is a sequence $w = w_1, w_2, \ldots, w_n$, trailed by an endless order of spaces B. TM container deliver and inscribe cyphers on the masking tape as it satisfies. Conversion role of TM is

$$\delta(q_i, a) = (q_j, b, \mathrm{R})$$

Turing Machine M adds a occupation f if, at what time the certain participation w is in the field of f, the apparatus breaks in its take public, with $f(w)$ in print on the parcel tape. For specimen, improve binary records, i.e., $f(m, n) = m + n$, then and there the amounts m and n remain to be hired on the adhesive tape as $0m10n$, somewhere 1 is a strainer for the figures m and n . Once handing out is finalized and the TM breaks then the insulating masking tape would require the guts as $0(m + n)$.

The combined 20 digit pin is encrypted using RSA algorithm and it is embedded in the palm print using Bits Wrap algorithm. Now the stego image of the palm print and the graphical image are stored in the data base. The stego image is that in which the data is hidden. Here for encryption 2 prime numbers are needed. One prime number is obtained from the user and the other prime number is defaultly generated. This is done, because the user does not clearly know which should be entered. So the user enters any number. If other number is a prime number and if both the numbers are multiplied, then the resultant number will be a prime number. So this procedure is followed.

2.2.1. RSA Algorithm

The RSA procedure is rummage-sale for together communal main encryption and numerical names. It is the maximum broadly castoff civic main encryption procedure. The base of the refuge of the RSA process is that it is precisely infeasible to issue satisfactorily great numbers. The RSA process is thought to be protected if its answers need a distance of at slightest 1024-bits.

Key Generation

RSA includes a civic crucial and a secluded key. The communal key dismiss be known to everybody and is castoff for scrambling communications. Letters converted with the municipal strategic can first be decrypted consuming the cloistered key. The sources on behalf of the RSA system are spawned the resulting manner:

1. Select two discrete primary records p and q.
2. Compute $n = pq$.
3. Subtract $\varphi(n) = (p - 1)(q - 1)$, everywhere φ is Euler's totient task.
4. Elect an numeral e such that $1e$, $\varphi(n)$ and highest mutual divisor of $(e, \varphi(n)) = 1$; i.e., e, $\varphi(n)$ remain positioned co prime.
5. Determine d as:

$$d \equiv e^{-1} (\text{mod } \varphi(n))$$

i.e., d is the multiplicative opposite of e mod $\varphi(n)$.

By construction, $d \times e = 1 \text{ mod } \varphi(n)$. The civic crucial involves of the modulus n and the communal exponent e. The sequestered key comprises of the modulus n and the remote champion which essential be reserved clandestine.

Encryption

The value of p and q are taken. Then the value of n is calculated. For example consider, $p = 3$ and $q = 11$. The value of $n = 33$. Then $\phi(n)$ is calculated as

$$(p - 1)(q - 1) = 2 \times 10 - 20.$$

The value of encryption exponent e is chosen as 7 as per this example. The cipher text c is given as,

$$c = m^e \text{ mod } \phi(n)$$

$$= 3^7 \bmod 33.$$

$$= 2187 \bmod 33 = 9.$$

Decryption

The value of m can be recovered since c by with the isolated key advocate d by computing,

$$m = c^d (\bmod n) \tag{5}$$

Given *m*, the unique communication M can be recovered by retrogressive the stuffing system.

2.2.2. Bits Wrap Algorithm

The knowledge late the Bits Wrap set of rules is to enclosure the bits of the unseen memorandum into the slightest morsels of the pixels. The planned scheme codes the facts with a crypto process and before inserts the coded facts in the palm print. This organization recovers the refuge of the facts by inserting the scrambled figures and not the unadorned records in the palm print. To insert a undisclosed letter in the protection sleeve secondhand two dissimilar devices: (1) code the underground memorandum (2) The scrambled top-secret note is embed in the asylum broadcasting by via bits wrap algorithm. The necessary clue at this time is to insertion the undisclosed letter in the smallest noteworthy whiles of the descriptions.

The palm print and the encrypted 20 digit pin is taken. The principal while of the pin is fixed into the principal pixel and the another bit is fixed into the another pixel therefore the resultant stego image is also an 8-bit gray ruler double and the variance amongst the refuge duplicate and the stego image is not visually appreciable. The palm print is taken and the pixels are chosen where the data is to be hidden. On the other hand the 20 digit code is converted into its binary form. The binary value along with the payload value which is 3 bits/pixel is wrapped into the lower nibble. The same process is continued for all the code bits. Then the palm is concealed with the data. Then the palm is deposited in the catalog.

2.3. Recognition Phase

Then during the recognition phase, the user is asked to choose the palm print and the graphical image and enter the pin that the user has chosen for enrollment phase. The landscapes of the palm print and the graphical image are extracted and are matched with that of the features of the palm print and the graphical image that are stored in the data base. If the geographies game, before the creature is said to be authorized. The matching process is carried out using Euclidean distance. If not the person is not authorized.

2.3.1. Euclidean Distance

Euclidean aloofness actions the likeness among two unlike mouth trajectories with

$$\mathrm{ED} = \sqrt{\sum_{j=0}^{\mathrm{J}} (\mathrm{FV}_{1,j} - \mathrm{FV}_{2,j})^2} \tag{6}$$

where J is the length of the feature vector, FV_i is the feature vector for individual *i*. Both of the nose trajectories is corresponding consuming Euclidean Distance with the lingering chin directions in the catalog.

The geographies of the tribute print in the data base are linked with that of the features of the palm print that are chosen by the user during recognition. The distance is calculated by the square root of the sum of the distances. The Euclidean distance is the short distance to the nearest pixel in the background.

2.4. One Time Click Image

Here before the enrollment phase, the person like admin has to click on a onetime click image. The one time click password stands an spitting image in which the user has to click on a particular point that is marked as the secret point. If anyone wrongly clicks on any other point in the image, then the user cannot enter for enrollment. And also at a time only one click is possible.

3. EXPERIMENTATION RESULTS

This section explains about the implementation results of this paper. The implementation has been performed in MATLAB. The results are as below.

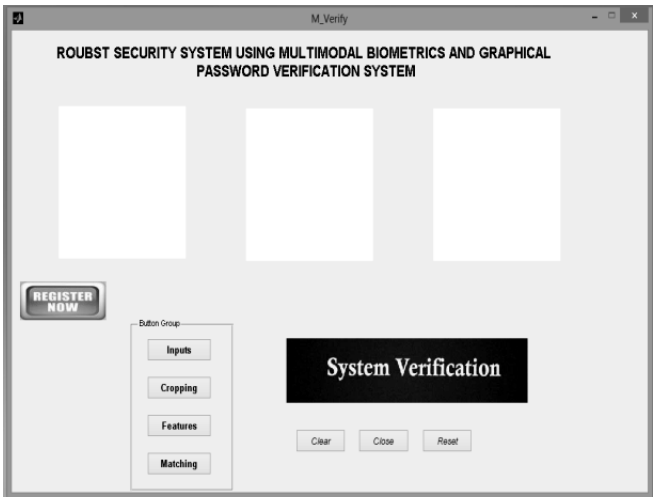

Figure 2: The enrollment screen

The user first has to click on the register now button for their enrollment.

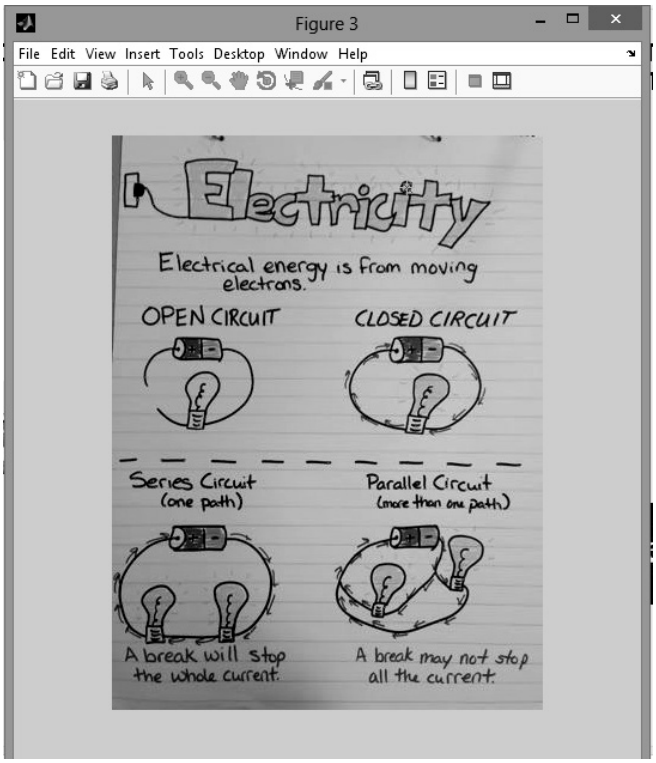

Figure 3: One time click image

The above screen is the one time click image in which the admin has to click on a particular point so that the user can enter for enrolling their palm print and graphical image.

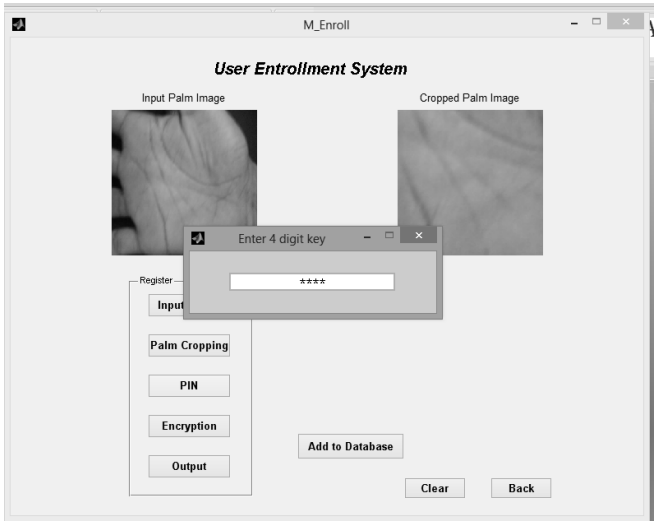

Figure 4: Entering of 4 digit pin

The palm print and the graphical image are chosen by the user. Here the user has to choose the palm print from a set of palm prints that are stored in the data base. But in real time, the user can take their own palm prints. The palm print is separated as blue plane and the palm print is cropped. And the user enters the 4 digit pin.

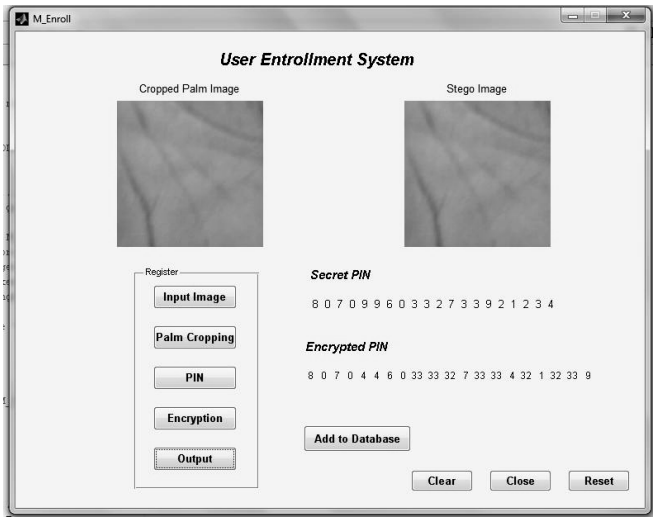

Figure 5: The encrypted data

The user entered 4 digit pin is combined with the 16 digit pin. And for encryption one of the numbers is entered by the user and the other number is generated automatically. And finally the encrypted pin is displayed.

After the embedded process, both the graphical image and the embedded palm print are stored in the data base.

After the features are extracted for the biometrics that are stored in the data base and the biometrics that the user chooses for their recognition, if the features matches then the user is authorized person as shown in Figure 7. If the features do not match, then it displays as unauthorized person. And it does not go for the next level.

Figure 6: The features are added to the data base.

Figure 7: Validating user

Figure 8: Final authentication

And finally, the user is asked to enter their 4 digit pin and the pin is decrypted and if it matches, then the user is said to be authenticated as shown in Figure 8.

4. CONCLUSION

In planned scheme, the multimodal biometrics with two different biometric features has been implemented. It overpowers the tricky of unimodal biometrics. Unlike other biometric system here the data is hidden

in the palm print. Before hiding the data, it is being encrypted and then hidden. And so, it is more secure than other biometrics system. The RSA process is secondhand for encryption. And so the data cannot be decrypted without a key. RSA algorithm is more secure so it is being used to surge the sanctuary of the undisclosed memorandum. And also before entering the system, the user has to come across a onetime click on a graphical image. And so if more than once the graphical image is clicked, then the user cannot enter the system. And more over, the user himself does not click on the image. There is a admin and he does this work. So it will be more secure than any other biometric system. For feature extraction, Weber's Local Descriptor is being used. It performs better than other feature extraction descriptors. And for recognition, the features have to be matched. For that Euclidean distance is used for matching. In future, other security based algorithms could remain rummage-sale to advance the recital. And also the combination of other behavioral and physical biometrics features could also be used.

References

1. Arun Ross, Anil Jain and Jian-Zhong Qian, "Information Fusion in Biometrics", Appeared in Proc. Of 3rd Int'l Conference on Audio and Video based Person Authentication (AVBPA), pp 354-359, Swedan, June 6-8,2001.
2. A. Annis Fathima, S.Vasuhi, N.T.Naresh Babu, V.Vaidehi , Teena Mary Treesa, " Fusion Framework for Multimodal Biometric Person Authentication System, IAENG International Journal of Computer Science, 41:1, IJCS_41_1_02, February 2014.
3. Manoj Kumar Sharma, Dr. Amit Upadhyaya, Shalini Agarwal, "Adaptive Steganographic Algorithm using Cryptographic Encryption RSA Algorithms", Journal of Engineering, Computers & Applied Sciences (JEC&AS) ISSN No: 2319-5606 Volume 2, No. 1, January 2013.
4. Shutao Li, Dayi Gong, Yuan Yuan, "Face Recognition Using Weber Local Descriptors", Neurocomputing 122(2013) 272-283.
5. Kaveh Ahmedi, Maral Mohamadi Zanjani, "A New Method for Image Security and Data Hiding in Image ", 2011 2nd International Conference on Business, Economics and Tourism Management IPEDR volume 24 (2011).
6. Babloo Saha, Shuchi Sharma, "Steganographic Techniques of Data Hiding using Digital Images", Defense Science Journal, Vol. 62, No. 1, January 2012, pp. 11-18, DOI: 10.14429/dsj.62.1436.
7. Rajan.S.Jamgekar, Geeta Shantanu Joshi, "File Encryption and Decryption Using Secure RSA, International Journal of Emerging Science and Engineering (IJESE) ISSN: 2319–6378, Volume-1, Issue-4, February 2013.
8. Ali E. Taki El_Deen, El-Sayed A. El-Badawy, Sameh N. Gobran, "Digital Image Encryption Based on RSA Algorithm, IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) e-ISSN: 2278-2834, p- ISSN: 2278-8735. Volume 9, Issue 1, Ver. IV (Jan. 2014), PP 69-73.
9. Jie Chen, Member, IEEE, Shiguang Shan, Member, IEEE, Chu He, Guoying Zhao, Matti Pietika¨ inen, Senior Member, IEEE, Xilin Chen, Senior Member, IEEE, and Wen Gao, Fellow, IEEE," WLD: A Robust Local Image Descriptor", IEEE Transactions On Pattern Analysis And Machine Intelligence, Vol. 32, No. 9, September 2010.
10. D. G. Agrawal, Pranoti M. Jangale, "Dynamic Texture Feature Extraction Using Weber Local Descriptor", International Journal of Scientific Engineering and Technology Research, ISSN 2319-8885 Vol. 03, Issue.03, March-2014, Pages: 0468-0471.
11. M.Brindha, Dr.G.M.Tamilselvan, Dr.S.Valarmathy, M. Arun Kumar, M.Suryalakshmipraba, "A Comparative Study of Face Authentication Using Euclidean and Mahalanobis Distance Classification Method", International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 1, January 2013).
12. Shailender Gupta, Ankur Goyal, Bharat Bhushan, "Information Hiding Using Least Significant Bit Steganography and Cryptography", I.J. Modern Education and Computer Science, 2012, 6, 27-34.
13. Sangita Nikumbh, Prerana Kamble, "Multimodal Biometric Security System with Steganographic Technique", International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064, Impact Factor (2012): 3.358.

14. Ogunlewe A. O, Adedoyin M. A, Folorunso C.O, "Science of Cryptography", International Transaction of Electrical and Computer Engineers System, 2014, Vol. 2, No. 2, 61-66.

15. Muhammad Hussain, Ghulam Muhammad, Sahar Q. Saleh, Anwar M. Mirza, and George Bebis, "Image Forgery Detection Using Multi-Resolution Weber Local Descriptors", EuroCon 2013 • 1-4 July 2013 • Zagreb, Croatia.

16. Hemalatha. S, U. Dinesh Acharya, Renukha. A, Priya R. Kamath, "A Secure Colour Image Steganography In Transform Domain", International Journal On Cryptography and Information Security(IJCIS), Vol. 3, No 1, March 2013.

17. Chiasson. S., et. al., "Multiple Password Interference in Text Passwords and Click Based Graphical Passwords", ACM, 2009.