INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

AN EXTENDED VISUAL CRYPTOGRAPHY WITH DYNAMICALLY AUTHENTICATED ERROR AVOIDANCE SCHEME FOR BANK APPLICATIONS

V. Suruthikeerthana[1], Dr. S.Uma[2]

[1] Student, Department of computer science and engineering, Hindusthan institute of technology, Coimbatore
[2] Head of the department, Department of Information Technology, Hindusthan institute of technology, Coimbatore

Abstract: - Visual cryptography is the most efficient and secured methodology to provide the authentication for the user who are accessing the system. Banking system is extended with the visual cryptography which is used to provide the secured authentication for the users who accessing the system. In the existing system, RGB based system is integrated with two share based scheme modules. It attempts to process the visual cryptography in the efficient manner. The scheme uses the secret image that is divided into a number of four channel images namely red channel, green channel, blue channel and alpha channel. Colour error diffusion technique is applied on each of the channel images. Channel images are divided into n number of shares, and the m number of shares that are used to extract the secret can be perfectly reconstructed and also when the complete knowledge of all the m-1 shares is revealed, no information about the original image can be obtained. This proposed methodology is extended to the finger prints that are unique for each person. Any Missing values of the shares leads to the failure of image authentication process. Thus in the proposed work, dynamic finger authentication scheme can be introduced which might lead to the successful authentication of the system in case of presence of missing share values too. From the experimental result, the conclusion decides that the proposed method is better than the existing system.

1. Introduction:

Image processing is utilized to convert an image into digital form and also performs certain operations on it, so that it gives an enhanced image. It is also used to extract certain useful information from the input image. The input can be an image or video frame or photograph and the desired output may be an image or characteristics associated with that particular image. Image Processing system usually treat the images as two dimensional signals and then apply the signal processing methods to the image. Rapidly growing

technologies today incorporate theses kind of technologies to be implemented, with its applications in various aspects of a business oriented accesses and thus it forms as a core research area within engineering and computer science disciplines.

Basic types of methods used for Image Processing are two, namely, Analog and Digital Image Processing. Analog or the visual techniques of image processing are used for the hard copies of applications like printouts and photographs. Digital Processing techniques help in the manipulation process of the digital images with the help of the computers. Raw data from the imaging sensors from satellite platform contains certain deficiencies. In order to avoid such problems and also to get originality of the information, processing is to be conducted at various phases. Pre- processing, enhancement and display, information extraction are the general three phases to be undergone.

Security is of utmost concern in today's world of growing technology. Cybercrimes had increased in time, so providing only the network security is not adequate. The Security provided to images like blue print of company projects, using image steganography and stitching and secret images of concern to the army or of company's interest is beneficial. When the text message encrypted using AES algorithm is embedded in a part of the image, secret message is difficult to be retrieved. Also when the secret image were broken down into parts and then sent to the receiver makes it difficult for the trespassers to get access to all the parts of the images at once.

Hence the security to an image must be increased to a higher level of processing techniques that becomes highly difficult for the intruder to detect and decode the document. No limitation on the image format, it can be a bmp or a gif image file, it can be grey scale or coloured images. Restrictions are on the size of the message needs to be of only 140 characters.

The Biometrics-based personal authentication systems which use physiological or behavioural traits are becoming popular when compared to the traditional systems which were based on tokens or knowledge. Daniele Gunetti [1] presented an analysis of keystroke as an authentication metric and Fabian et al [2] proposed authentication using keystroke dynamics. And also long text input keystroke was involved to authenticate the users [5].

Biometric authentication systems can be more flexible for the users because there is no need of password that can be forgotten or a key that can be lost and it just needs a single biometric trait to access several accounts without the burden of remembering passwords. Even it has numerous advantages; they are vulnerable to attacks that can decrease their security.

2. Related Works

Ratha et al [3] analysed these attacks, and grouped them into eight classes. The Type 1 attack involved the presence of a fake biometric to the sensor. A previously intercepted biometric which was submitted, constitutes the second type of attack. The third type of attack is that the feature extractor module was compromised that produce feature values selected by the attacker. The fourth type of attack include when the genuine feature values are replaced with the ones that are selected by the attacker. Then the fifth type of attack was that the matcher can be modified such that it provides an output as an artificially high matching score. The attack on the template database constituted for the sixth type of attack. The seventh type of attack includes the transmission medium between the template database and the matcher is attacked and thus resulting in the alteration of the transmitted templates. Finally, the result of the matcher was overridden with the attacker.

Maltoni et al. [4] discussed about the problems of a generic authentication application that result in quite different effects for the traditional biometrics-based systems. An attacker corrupts the authentication system such that legitimate users cannot use it in Denial of Service (DOS). In case of a biometric authentication system, an online authentication server processes access requests using the retrieving templates from a database and perform matching process. It was bombarded with many bogus access requests, to a status that the server's computational resources cannot handle valid requests any more.

Messerman et al [6] improved the existing keystroke dynamics based verification schemes on four aspects. Initially, scalability was improved with a constant number of users instead of whole user space

that verified the identity of the target user. Then, an adaptive user model was provided that enabled the solution to consider the change of user behaviour in the verification decision. Then, a new distance measure was identified to verify the identity of a user with shorter text and finally, the number of the false results was decreased. This proposed solution was evaluated on a data set collected from users while they were interacting in mail-boxes and also during their daily activities. The main drawbacks are Acceptance problem occurs because of low error results and the Solution must be evaluated for internal and external attackers.

Umut Uludag et al [7] proposed an attack system using hill climbing procedure to synthesize the targeted minutia templates. Its feasibility was evaluated with sufficient experimental results conducted on a large database of fingerprints. The probability of such attacks was decreased using several measures and their ramifications were also presented. Maxion et al [8] proposed the concept of Keystroke dynamics for the identification of the individual users on the basis of their typing rhythms derived from the timestamps of key-press and key release events. 28 users typed the same 10-digit number, using only the right-hand index finger. The main disadvantages are Very hard to compare results in keystroke experiments. An equal-error rate (EER) does not admit the details of the trade-off between misses and false alarms. Lower cost-of-error score for the classifier/detector was detected.

Lívia C. F. Araújo et al [9] used a static keystroke dynamics in user authentication. The inputs to the system are the key down and up times and also the key ASCII codes captured while the user types a string. The four features namely key code, two keystroke latencies, and key duration were analyzed and about seven experiments were performed combining these features. The results of the experiments were evaluated the legitimate, the impostor and the observer impostor users.

Lucas et al [10] described steps toward developing evaluation methodologies for behavioral biometrics that take into account threat models that have been largely ignored. Handwriting was taken as a point that some users are significantly better forgers than others. Such forgers were trained to pose a greater threat, because certain users are easy targets for forgers, and that most of the humans hold relatively poor judgement of handwriting authenticity. Additionally, in order to overcome the labor-intensive hurdles for performing more accurate assessments of system security, a generative attack model was proposed based on concatenated synthesis which provides a rapid indication of the security afforded by the system. However, the system has high computational complexity.

In Patrick et al [11] different distance metrics can be used in this process, like Euclidean, Normalized Bayesian Classifier, or Time Classification. The authors consider keystroke dynamics on free text and also the statistical properties of the combinations of two to four letters. This approach was the first step towards the real continuous authentication, but they finitely look at specific character combinations from various users which is a tedious process and time consuming.

Lucas et al [12] proposed Randomized Biometric Templates (RBTs) that are used by legitimate users to create keys. It was designed in a way so that attackers were not able to gain the knowledge of biometric input measurement. The RBTs assigned different features to different users, and also encoded the features so that attackers could not determine which features were originally used to generate a key. The utility of this approach is two-fold where first; it increased the work required for correct key search because the attacker has to find both the set of features that were used, and also the correct biometric sample. Then it assigned only strong features to each user such that the attacker must had to make a perfect guess of the biometric input in order to correctly hack the key. However, only limited information from a target user should be taken and performance against attacks must also be improved.

Lucas et al [13] presented a study of threat models. Some of the attacks are more realistic than others; all are designed to “stress” handwriting biometrics in a variety of new metrics. The proposed work had ultimate to build confidence in the inherent security of a given measure. The proposed model was demonstrated and trained only on captured static samples combined with the pen-stroke dynamics was nearly as effective as the best human forgers have encountered. Lack of accuracy and limited number of samples are the limitations in this work.

3. Existing System

Signature data was collected from 30 participants in the existing system. Each participant was asked to sign their names as consistently as possible ten times. Most of the participants those who have not used a tablet PC before, lose consistency in their signature and so some participants were allowed to sign a word instead. Then the network was tested on 3 among the user's signatures that were not indulged in the training phase of the system. Same process was repeated 5 times for each user and the results were gathered and also were repeated with fast Fourier transformations and the Derivatives. They were tested with and without noise generation also. Network's other features were tested by experimentation.

Algorithm which was explained is improved by the processing of the signature of the applicant Signature is fetched as an input and is divided into different number of shares depending upon the banks scheme system. One of the shares is preserved in the bank database and all other shares are given to the applicant. During every transaction, the applicant has to provide his shares and those shares are over lapped with the already existing bank shares. This process is done as a check for authentication with the help of correlation technique. The authentication is succeeded only when higher correlation coefficient is achieved. The main drawback in the system is that Colour images cannot be supported well and better coherence value cannot be achieved. In order to meet these challenges, a proposed method is introduced.

4. Proposed System

The overall process of Dynamically Authenticated Error Avoidance Scheme consists of several steps which are explained as follows. A secret image which may be a fingerprint is divided on the basis of four channels and the image is encrypted with the help of error diffusion technique. The technique follows a grey scale value as a threshold. The process of encryption is also made hybridized with the dynamic authentication scheme. Then the image is decrypted and forwarded for the access of the users.

Proposed Algorithm of Dynamically Authenticated Error Avoidance Scheme:

Input: Original Image

Output: Encrypted Image

1. Extract the image of the corresponding user from the database, and the original image be G;
2. The user selects the password and identity that is it may be an image type.
3. Generate four channel images from the original image

   $G = G_r + G_g + G_b + G_a$
4. Size of the image is [M, N], M is the rows and N is the number of columns.
5. For rows 1 to m and cols=1 to N ;
6. **Encryption through Error Diffusion**: Scan all the pixel in matrix in a raster scan order starting from pixel up to the left and goes through all pixels in the matrix.
7. If G(rows,cols)≥127.5) grey scale index value is 127.5;

   set K(rows,cols)=1

   else

   set G(rows,cols)=0
8. Since all pixels in G which are real numbers from 0 to 255 has been replaced by 0 and 1 in new K image matrix and the error value is calculated as:

   E= G(rows,cols)-k(rows,cols)

   The error E is difference between the pixels value in G and K matrix of the image at that particular position.
9. The error occurred at the position of a pixel is weighted by a value 0.075 and it is added to pixel at (rows,cols+1).
10. After the error is diffused, the pixel value of next position is compared to the threshold and same process continues until all pixels aredone.
11. end of for loop
12. end of for loop

13. **Encryption through Dynamic Authentication** using the password and the session ket generated.
14. Apply (2,2) visual sharing scheme, where binary image of size 100X100 has been considered in our design where each pixel is either 0 or 1.
15. The four shares are also encrypted using the 8 bit LFSR by XORing the share bit with the LFSR bit, then it is repeated for the whole image.
16. Encrypt the image using the shares that are obtained in previous step
17. Generate the keys and send it to receiver for decryption.
18. Extract the keys to decrypt the original image
19. Decrypt it using (2,2) visual cryptography
20. Decrypt again using the user generated key and the bitwise ORed shares.
21. Stack the shares
22. Retrieve the original image.

Algorithm Description:

A secret image is divided into four channel images namely red channel, green channel, blue channel and alpha channel. Error diffusion technique is applied on each channel. Respective channel images are further divided into n number of shares such that even with any number of shares say m, the secret can be perfectly reconstructed. The security must be in a way that even the complete knowledge of m-1 shares does not reveal any information about the original image.

Error diffusion technique is a type of half toning where the quantization residual is given to neighbouring pixels which have not yet been processed. The algorithm scans the image one row at a time and one pixel at a time with a basic process. Current pixel under consideration is compared to a half-grey value. If it is above that particular value, a white pixel is generated in the resultant image. Either if the pixel is below the half way brightness value, a black pixel is generated there. Thus the generated pixel is either fully bright or fully black. The error is then added to the next pixel in the image and the process repeats. This image is suggested to further encryption by the use of dynamic authentication scheme where the authentication becomes more secure and efficient.

The shares that are obtained after the application of proposed diffusion technique are enveloped with the help of innocent covers using invisible digital watermarking. Thus the encrypted image is produced after his process. The key which is generated consists information on the number of shares and the information about the envelop images in the process.

In the decryption process, it involves the retrieval of the key at the receiving side and also the information about the number of shares and the envelop images used to watermark. Once the key is retrieved, the enveloped images are identified and the watermark is removed from the shares. Shares are stacked together using XOR operation to produce better quality of decrypted image. Channel images are thus obtained and are superimposed to get the original image. Process of decryption is the reverse process of the encryption. The shares are stacked together and also the 2×2 block is sub sampled into a single pixel and the size of the decrypted image is same as the size of the original image. The main advantage of the system is it achieves better coherence value and also support for colour images. The description on each stage is given below,

The proposed scheme has the following main advantages;

(1) A user can easily choose a password and identity.

(2) It can guarantee perfect session key forward secrecy, and

(3) It does not maintain a verification table.

As a result, our proposed scheme can provide greater security and be practical in wireless communication systems.

Results and Discussion

Performance evaluation of the proposed research scenario called An Extended Visual Cryptography with Dynamic Authentication Scheme is performed and its results are compared with the existing research

work. This comparison is made against the parameters called the accuracy, precision, recall and the F-Measure. These metrics are defined and the true values obtained in both research scenarios are given detailed in the following sub sections.

Accuracy Comparison

$$\text{Accuracy} = \frac{(\text{True positive}+\text{True negative})}{(\text{True positive}+\text{True negative}+\text{False positive}+\text{False negative})} \quad (4)$$

Comparison of the accuracy parameter value between the existing and proposed research scenarios is depicted in the graphical representation as like follows:

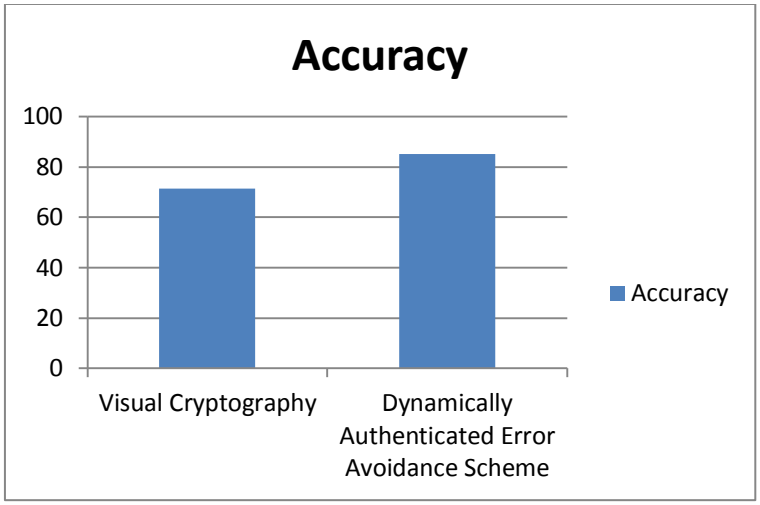

Figure 1. Accuracy comparison

In the figure 1, methodologies are depicted in the x axis, and the accuracy values obtained for those methodologies are given in the y axis. From this graph, it is proved that the proposed research scenario is improved in its performance than the existing research scenarios.

Precision Comparison

Precision value is determined based on the retrieval of information at true positive prediction, false positive. Precision is determined the percentage of positive outcome returned that are relevant.

Precision =TP/ (TP+FP) (5)

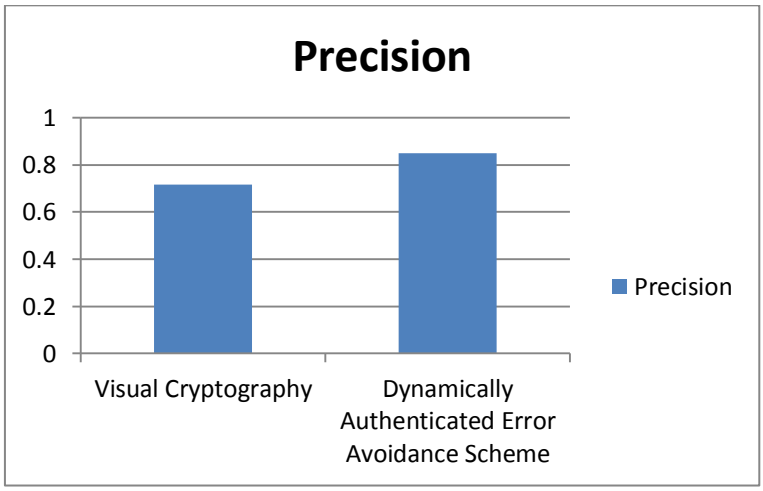

Figure 2. Precision comparison

Comparison of the precision parameter value between the existing and proposed research scenarios is depicted in the graphical representation given above.

In figure 2, methodologies are depicted in the x axis, and the precision values obtained for those methodologies are given in the y axis. From this graph, it is proved that the proposed research scenario is improved in its performance than the existing research scenarios.

Recall Comparison

Recall value is determined based on the retrieval of information at true positive prediction, false negative. Recall in this context is also referred to as the True Positive Rate. In that process the fraction of relevant instances that are retrieved.

$$\text{Recall} = TP / (TP+FN) \qquad (6)$$

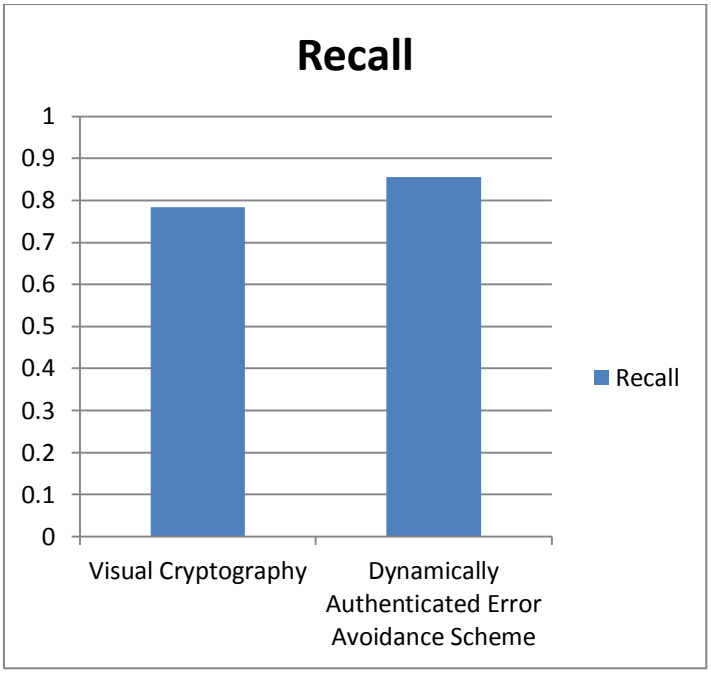

Figure 3. Recall comparison

In the above figure, methodologies are depicted in the x axis, and the recall values obtained for those methodologies are given in the y axis. From this graph, it is proved that the proposed research scenario is improved in its performance than the existing research scenarios.

F-Measure Comparison

The F-Measure computes some average of the information retrieval precision and recall metrics

$$\text{F-measure} = \frac{2 * \text{precision.recall}}{\text{precision} + \text{recall}} \qquad (7)$$

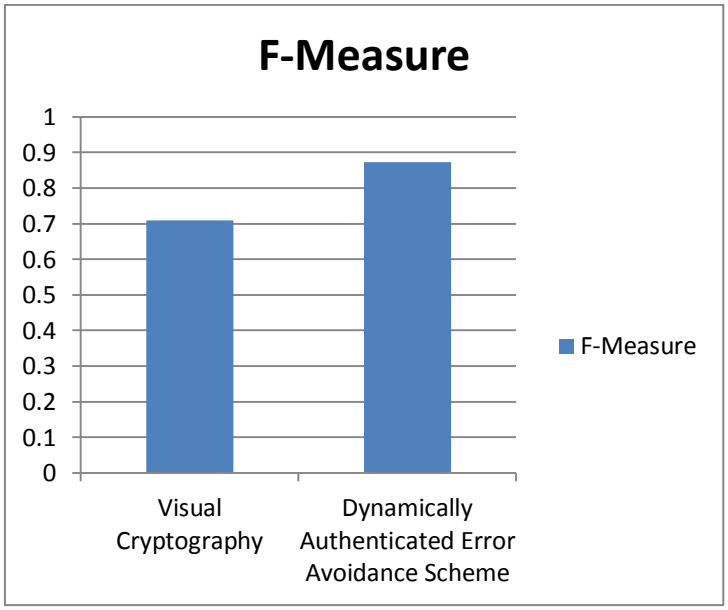

Figure 4. F-Measure comparison

In the above figure, methodologies are depicted in the x axis, and the F-Measure values obtained for those methodologies are given in the y axis. From this graph, it is proved that the proposed research scenario is improved in its performance than the existing research scenarios. The actual values that are obtained for the performance metrics are given in the following table.

Table 1. Comparison of Parameters

Parameters	Visual Cryptography based Authentication	Dynamically Authenticated Error Avoidance Scheme
Accuracy	71.25	85
Precision	0.7159	0.8499
Recall	0.7845	0.856
F-Measure	0.7094	0.8721

Conclusion and Future Work

Secure bank authentication plays a great role in the many of the real world application where the consumers start to do their transaction in the online manner. In this work, secure bank authentication is introduced for ensuring the secured environment for the users. The security is further improved in the scenario by introducing the secure sharing of keys in terms of stacking and key generation approach with the error diffusion and the dynamic authentication scheme compositely called as Dynamically Authenticated Error Avoidance Scheme. In the proposed research colour images are supported for the efficient authentication process. The experimental tests conducted were proves that the proposed approach leads to a better result than the existing work in terms of improved accuracy. As a future research multi biometric based authentication can be introduced that attempt to provide the secured environment for the banking users. Threshold based user authentication can be introduced where the valid user authentication would be spoiled in case of corruption of any shares.

REFERENCES

[1] D. Gunetti and C. Picardi, "Keystroke analysis of free text," ACM Trans. Inf. Syst. Secur., vol. 8, no. 3, pp. 312–347, Aug. 2005.
[2] F. Monrose and A. Rubin, "Authentication via keystroke dynamics," in Proc. 4th ACM Conf. Computer and Commun. Security, NY, USA, 1997, pp. 48–56.
[3] N.K. Ratha, J.H. Connell, and R.M. Bolle, "An analysis of minutiae matching strength", Proc. AVBPA 2001, Third International Conference on Audio- and Video-Based Biometric Person Authentication, pp. 223-228, 2001.
[4] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, Springer, 2003.
[5] R. S. Zack, C. C. Tappert, and S.-H. Cha, "Performance of a long-textinput keystroke biometric authentication system using an improved k-nearest-neighbor classification method," in Proc. 2010 Fourth IEEE Intl. Conf. Theory Applications and Systems (BTAS), 2010, pp. 1–6.
[6] Messerman, T. Mustafić, S. A. Camtepe, and S.Albayrak, "Continuous and non-intrusive identity verification in real-time environments based on free-text keystroke dynamics," in Proc. IEEE Int. Joint Conf. Biometrics (IJCB 11), Oct. 11–13, 2011, pp. 1–8.
[7] U. Uludag and A. K. Jain, "Attacks on biometric systems: A case study in fingerprints," in Proc. SPIE Security, Steganography and Watermarking ofMultimedia Contents VI, Jan. 2004, vol. 5306, pp. 622–633.
[8] R. Maxion and K. Killourhy, "Keystroke biometrics with number-pad input," in Proc. 2010 IEEE/IFIP Int. Conf. Dependable Systems and Networks (DSN), pp. 201–210, 28 2010-July 1 2010.
[9] L. C. F. Araujo, L. H. R. Sucupira, M. Lizarraga, L. Ling, and J. B. T. Yabu-uti, "User authentication through typing biometrics features," IEEE Trans. Signal Process., vol. 53, no. 2, pp. 851–855, Feb. 2005.
[10] L. Ballard, D. Lopresti, and F. Monrose, "Forgery quality and its implications for behavioral biometric security," IEEE Trans. Syst., Man, Cybern. B, vol. 37, no. 5, pp. 1107–1118, Oct. 2007.
[11] D. Gafurov, E. Snekkenes, and P. Bours, "Spoof attacks on gait authentication system," IEEE Trans. Inf. Forensics Security, vol. 2, no. 3, pp. 491–502, Sep. 2007.
[12] L. Ballard, S. Kamara, F. Monrose, and M. K. Reiter, "Towards practical biometric key generation with randomized biometric templates," in Proc. 15th ACM Conf. Computer and Communications Security, New York, NY, USA, 2008, pp. 235–244.
[13] L. Ballard, D. Lopresti, and F. Monrose, "Evaluating the security of handwriting biometrics," in Proc. 10th Int. Workshop on the Foundations of Handwriting Recognition, 2006, vol. 15, pp. 461–466.
[14] L. Ballard, F. Monrose, and D. Lopresti, "Biometric authentication revisited: Understanding the impact of wolves in sheep's clothing," in Proc. 15th Conf. USENIX Security Symp., California, USA, 2006, vol. 15.