Integrating Cancellable Biometrics with Geographical Location for Effective Unattended Authentication of Users of Mobile Devices

Hisham Al-Assam, Ihsan A. Lami, and Torben Kuseler
Applied Computing Department, University of Buckingham, Buckingham, MK18 1EG, UK
Email: hisham.al-assam@buckingham.ac.uk; ihsan.lami@buckingham.ac.uk; torben.kuseler@buckingham.ac.uk

***Abstract*—**Over the past decade, security and privacy concerns about the growing deployment of biometrics as a proof of identity have motivated researchers to investigate solutions such as cancellable biometrics to enhance the security of biometric systems. However, the open nature of newly emerged mobile authentication scenarios has made these solutions impractical and necessitated the need for new innovative solutions. This paper proposes an effective authentication scheme for remote users on mobile-handsets. The proposal incorporates cancellable biometrics with actual mobile-handset location to produce a one-time authentication token. For added security, the location is obtained and verified via two independent sources, and the authentication token is robustly stamped by the transaction time to guarantee the liveliness. This makes the proposed scheme immune against replay and other remote fraudulent attacks. Trials and simulations based on using biometric datasets and real GPS/Cellular measurements show the viability of our scheme for unattended and mobile authentication.

***Index Terms*—**mutual authentication, biometrics, location verification, multi-factor authentication

I. Introduction

Mobile transactions are becoming part of everyday life, enabling financial and other sensitive transactions to be performed anywhere, anytime by anyone. From a security perspective, this continuous mobility of the user has made the user authentication task more difficult and encouraged identity theft criminals. This is due to the fact that the important authentication components of "who, where and when" that were clearly defined in an office-based, face-to-face authentication process do no-longer exist in unattended, remote and mobile authentication scenarios. i.e. no direct and immediate credentials can be authenticated. For example, mobile banking (transferring money or paying bills) has become one of the most popular financial applications on Smartphones. Some time ago, a client had to go to his/her bank branch, fill-out a paper form, sign it and hand it to the bank clerk in person to pay a bill via bank transfer. Nowadays, all this can be done easily whilst on the move using a Smartphone application. However, in these mobile application scenarios, the authenticator can only base the authenticity decision (i.e. is a genuine client performing this transaction) upon the remotely received user authentication factors. This introduces new challenges to the authentication process as well as the authentication factors (PIN, Token) adopted.

In general, traditional authentication factors can be broadly categorised into three groups [1]:

1) Knowledge-based, or "something you know," e.g. a Password or PIN.
2) Object-based, or "something you have," e.g. a physical token like an ATM or credit card.
3) Identity-based, or "something you are," i.e. biometrics, which relies on the uniqueness of physical or behaviour characteristics of a person such as fingerprint, facial features, iris, or voice.

Biometric-based authentication offers an advantage over the other traditional authentication factors in a way that a legitimate client does not need to remember or carry anything. Furthermore, biometric-based authentication is known to be more reliable than traditional authentication due to the fact that it is linked with the identity of individuals. However, biometric systems are not perfect and their security can be undermined in different ways. For example, biometric data such as face images or fingerprints is not secret, and such biometric samples can be captured without individual's knowledge. Moreover, a biometric template can be replaced by an impostor's template in a system database or it might be stolen and replayed [2].

Multi-factor cancellable / revocable biometric authentication has been proposed to remedy some of these aforementioned drawbacks of biometric only systems as well as to enhance the security and/or accuracy of biometric authentication systems [3], [4]. However, cancellable biometrics is not immune to replay attacks and unless other authentication factors are incorporated in the authentication process, this could become a source of fraud. Therefore, this paper concludes that proper incorporation of further authentication factors like a time and location stamp can prevent replay attacks and also enhances robustness of the authentication system against fraud.

State-of-the-art generations of mobile-handsets (e.g. Smartphones like the iPhone5 or Samsung Galaxy S4) feature a wide variety of sensors (cameras, microphones, touch-pads, etc.) and wireless transceivers (Bluetooth,

Manuscript received June 1, 2013; revised October 31, 2013.
Corresponding author email: hisham.al-assam@buckingham.ac.uk.
doi:10.12720/jcm.8.11.780-787

Wi-Fi, Cellular, etc.) as well as GNSS receivers (GPS, Glonass and Galileo) that can be used to obtain further information about the mobile-handset user and his current environment. Recently, for example, clients' location has been introduced as a new authentication factor that can be easily obtained using the onboard GPS receiver. However, it is arguable if location alone can uniquely recognise/identify individuals [5].

Therefore, the scheme proposed in this paper combines several authentication factors to produce a single multi-factor representation (called mFactor in the remainder of this paper) of any client to enhance the reliability of the authentication data and consequently strengthen the overall transaction process. The authentication factors securely combined by this scheme to the mFactor are biometric data, passwords, PINs, a token, as well as real-time and geographical location of the client's mobile-handset. Integration of Time and Location (T&L) serves two main purposes. "Time" is used to stamp the client's authentication data representation to guarantee the one-time property (or liveliness) of the authentication message and therefore prevents replay attacks. "Location" contributes to authenticate the physical presence of the client (mobile-handset owner which need to be registered at the authenticator). To safely verify the claimed client's location, it is important that a second independent location source is used [5]. This minimises the risk that an adversary masquerading his/her real location.

The rest of the paper is organised as follows. Section 2 presents a review of the background of the main elements of the proposed authentication scheme. Section 3 presents the proposed scheme, while section 4 is devoted to the implementation and simulation work carried out. Section 5 draws the final conclusion.

Please note that in what follows, the "Client" refers to the person who needs to be authenticated remotely while using a mobile-handset (e.g. Smartphone). The "Authenticator" refers to the establishment (e.g. Bank or Certification Authority), which already holds the client's matching authentication data collected during an "enrolment" stage and also offers the agreed authentication process.

II. Background

This section provides background information on the main elements of the proposed scheme, and presents relevant work from the literature.

A. Location Authentication using Two Independent Sources

In mobile transactions, verifying the current position of the mobile-handset is useful to optimise the service, enhance security, and provide non-repudiation. In this proposed scheme, we use two "independent" sources to verify the client's claimed location. This is a) to prove that the client is within a certain area and b) to enable the authenticator to actually authenticate the location of the mobile-handset used in the transaction. The use of a second, different positioning technique, which is completely independent from the localisation method used onboard the mobile-handset itself, can be used to solve this so called "in-region" verification problem [6]. In an "in-region verification problem," an authenticator wants a proof that the user is within a claimed area. This is in contrast to the "secure location determination problem," where the authenticator wants to discover the location of a client without any further knowledge about the location and independently from any previous location claims made by the client. In mobile transaction scenarios that are targeted by this proposed scheme only the former "in-region" verification problem is relevant, because the previously claimed location of the client needs to be verified by the authenticator. Please note that, different positioning / localisation techniques (e.g. GPS, Wi-Fi Access-Point or cellular network based positioning) can be used as long as the used techniques are independent from each other as well as the technique that is used to verify the claimed position is not easily forgeable or manipulable by the mobile-handset user, i.e. the property of independent remote-positioning must be preserved.

The use of two independent sources of positioning to enhance remote authentication was introduced by the authors in [7]. This scheme elaborates on this methodology, and presents a practical implementation level to be used in applications that require unattended and mobile authentication with strong security and client privacy.

B. User-Based Random Projection (UBRP)

UBRP is a technique that uses Random Orthonormal Matrices (ROMs) to project existing data points into other spaces, ensuring that the distances between all the data points before and after the transformation are preserved [8]. UBRP is used in this scheme as a secure transformation for biometric templates to meet the revocability property for biometric-based authentication systems [4], [8]. Typically, UBRP is applied in two stages:

1) Generate a user-based orthonormal n x n matrix A, where n is the size of biometric feature vector.
2) Transform the original template feature z to a secure domain using matrix product y=Az.

Random Orthonormal Matrices are often generated from a user-based key (based on a password/PIN or token) using the Gram-Schmidt algorithm [4]. However, a more efficient and stable method to construct UBRPs is by using block diagonal matrices of small size rotation matrices [8].

C. Error Correcting Codes (ECCs)

Biometric data is "fuzzy" due to the differences between the client's captured biometric sample on the mobile-handset and the previously enrolled biometric sample stored by the authenticator. The variance of

biometric feature vector samples belonging to the same person can be considered as "noise". Therefore, Error Correcting Codes (ECCs) can be used to eliminate the effect of this noise [9]. In biometric-based authentication, an ECC encoding algorithm is carefully selected after analysing error patterns of inter-class and intra-class variations of biometric samples. In other words, the selected ECC should tolerate (correct) up to a fixed number of bits (threshold). This threshold should be carefully chosen to balance the trade-offs between False Acceptance Rate (FAR) and False Rejection Rate (FRR).

III. The Proposed Approach

This section is dedicated to describe the proposed approach for combining cancellable biometric data with time and location to be used for unattended and mobile authentication.

A. Thread and Trust Model

The subsequent thread and trust model is assumed for the proposed scheme and involves the following four parties:

1) The authenticator, who offers a remote service or mobile application that requires secure authentication of any previously registered client.
2) The client, who uses the application typically provided by the authenticator on his/her mobile-handset to access the services. The client must have a previously established business connection with the authenticator and has also previously registered and enrolled all required authentication credentials and personal information (e.g. PIN and biometrics).
3) The adversary, who illegitimately wants to use the protected service or the mobile-handset application.
4) The cellular Mobile Network Operator (MNO), who services the client's mobile-handset and handles the mobile network communication. The MNO also determines the client's current mobile-handset location via trilateration during normal operation [10]. The determined mobile-handset location is communicated to the authenticator to be used for independent verification of the client's claimed location.

The proposed scheme assumes the following trust model between these four parties:

1) The client trusts the authenticator to provide correct functioning mobile applications. Furthermore, the client trusts the authenticator to handle all previously registered and enrolled sensitive client data (e.g. biometrics) correctly. The client also trusts the authenticator to have robust security and privacy mechanisms, as for example described in [11], in place.
2) The client trusts the MNO to handle the mobile communication correctly.
3) Both, client and authenticator, trust the MNO to determine and report the client's current mobile-handset location to the authenticator accurately.
4) The authenticator does not trust any authentication data received from the client. Specially, the authenticator does not trust the client's claimed location and uses the mobile-handset location provided by the MNO to independently verify the client's location claim.

B. General Process of the Proposed Scheme

Prior to the first use of this authentication scheme, clients have to enrol their cancellable biometric template, shuffling key, and areas of operation with the authenticator. Enrolment of the areas of operation (i.e. regions in which the client can use the application) is optional in this scheme. If this feature is used, then the client is limited to these pre-agreed regions and would not be able to use the application outside. This enhances the security because an adversary could not use the application in "unusual places," for example in a different country. This feature is similar to blocking ATM transactions outside the home country as performed nowadays by various banks. However, as this feature clearly restricts the "mobile nature" of mobile-handsets, if is integrated only as an optional feature and can be down off, if the client wishes to do so.

The actual authentication process, as illustrated in Fig. 1, starts with the mobile-handset GPS/Wi-Fi receiver obtaining live GPS/Wi-Fi $T\&L_C$ data, which then gets converted to binary. Please note that the subscript C denotes data obtained by the client, whereas subscript A denotes data obtained by the authenticator in Fig. 1. The resultant concatenated binary representation of $T\&L_C$ is then shuffled by a shuffling key coming from a password/PIN entered by the client or token stored on the mobile-handset. The resultant code is encoded using an ECC. The ECC is used to eliminate the effect of the noise of the biometric data, which allows the authenticator to retrieve $T\&L_C$ captured at the client side from the data-message. Concurrently, a real-time, fresh biometric sample of the client is captured using one or more of the mobile-handset sensors (camera, microphone, etc.). After extracting the client's Biometric Feature Vector (BVF), this scheme applies the UBRP followed by a biometric "binarisation" on the data to produce a "Cancellable Biometric Binary Representation" (CBBR) of the client. Finally, the output of the ECC encoder is XORed with the CBBR to produce the mFactor, which is then sent to the authenticator for verification using a secure, wireless communication link.

When the authenticator receives the client's authentication message, the stored cancellable binary biometric template is retrieved from the authenticator's database and XORed with the received mFactor. The output is then fed to a local ECC decoding process to correct the bits resulting from the difference between the enrolled and the freshly captured biometric samples. Note that, both the client and authenticator use the same type of ECC in this scheme. If the difference is too big to be tolerated, then the authenticator concludes that someone

else is trying to imposter the genuine client, and the authentication attempt is rejected.

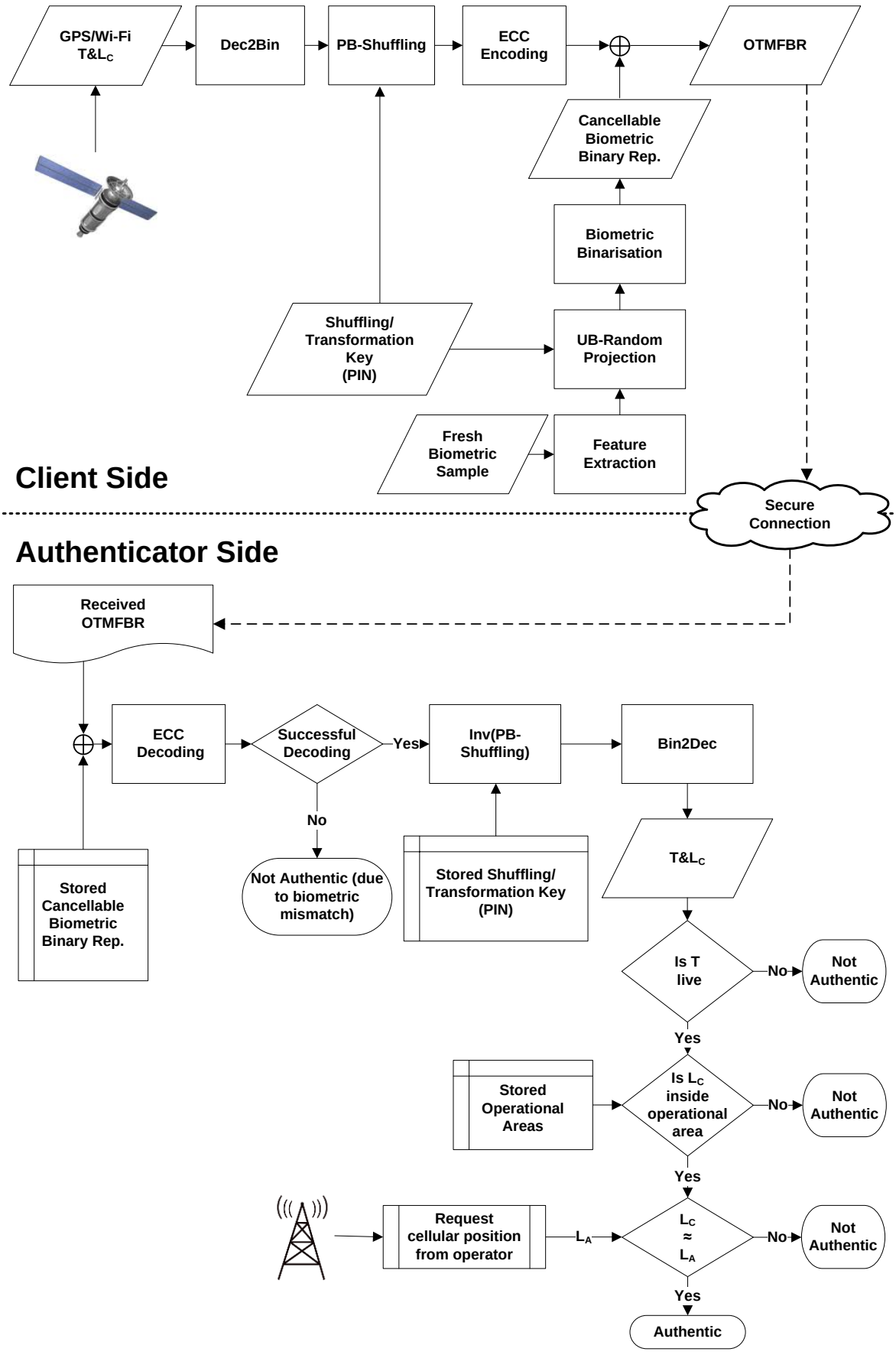


Figure 1. The proposed scheme

If the biometric verification is passed, then the inverse shuffling is applied on the decoded data to re-produce the binary representation of the GPS/Wi-Fi $T\&L_C$.

The result is then converted back into its original decimal representation. Obtaining valid time and location means that the client has used the genuine shuffling key. In addition, the authenticator will verify the liveliness of the mFactor by comparing the resulting GPS/Wi-Fi time TC with the current time TA. If the difference between the two timestamps is greater than a specific, pre-defined threshold, then the authentication attempt will be considered as a "replay attack" and consequently rejected. After passing the liveliness criteria test, the authenticator proceeds with verifying the claimed/received GPS/Wi-Fi position LC by requesting the client's location LA independently from the MNO. Finally, if LC is inside the operational area in the case this optional feature is used, and the distance between LC and LA is within a specific, pre-defined range, the authentication attempt is approved by the authenticator and the transaction with the client will continue.

IV. Implementation & Discussion

In the experiments and trials carried out to test the viability of this scheme, it has been decided to tolerate a difference of up to 320 meters between the locations provided by the two independent localisation techniques. This distance is so chosen because the FCC E911 [12] directive requires the MNO to be able to report the actual position of any mobile-handset within 300 meters accuracy in 95% of all cases.

Face biometric is selected for the implementation due to the camera availability on today's available mobile-handsets to capture the client's face images. Discrete Wavelet Transform (DWT) using the Haar filter is selected as an efficient tool to extract the facial features from these images [13]. The used size of facial feature vector extracted by DWT is 504-features in the experiments. A cancellable version is then created using UBRP. The biometric binarisation, as shown in Fig. 1, produces a 504-bit cancellable face representation. By analysing the error patterns of inter- and intra-class variation of face images using the training image samples, it has been decided that 38% of the binary face feature vectors needs to be corrected, or 191 out of 504-bits. In other words, if the Hamming distance between two binary feature vectors is less than 191, then the two feature vectors are accepted as belonging to the same client.

To deal with intra-class variations of face samples, the Reed-Solomon RS(511, 129, 191) ECC was used. This ECC takes 129 symbols as input to produce a codeword of 511 symbols, and therefore corrects up to 191 errors. The final mFactor is then obtained by XORing the ECC encoding codeword output with the 511-CBBR. We refer the reader to [9] and [14] for further details on using ECC for correcting the errors resulting from intra-class variations of biometric systems.

A. Experimental Datasets

Two main datasets were used in the experiments: a) the biometric dataset based on the Extended Yale-B database [15] and b) the location dataset collected by the authors in the city of London, UK.

The Extended Yale-B database has 38 subjects. Each subject, in frontal pose, has 64 images captured under different illumination conditions. Hence, the total number of frontal face images in the database to be used in the experiments is 2432. These images are divided into five subsets according to the direction of the light-source from the camera axis.

The location dataset contains 20 measurements. An Samsung Galaxy mobile-handset running the Android OS was used to collect the GPS-based location data. The cellular network (MNO tower-based) location of the mobile-handset was requested from the "mobile phone tracking service FollowUs" [16] .

All combinations of the 38 subjects and the 20 location measurements were considered in the experiments, i.e. each subject with all the 20 locations. The tolerance level between GPS- and tower-based localisation (320 meters) was chosen independently from the collected location dataset.

Table I shows some examples of the taken location measurements in terms of longitude and latitude values. Loc_{GPS} represents the measurements taken by the client on his mobile-handset. Loc_{Tower} represents the measurements requested from the MNO. The last two columns in Table I show the difference between Loc_{GPS} and Loc_{Tower} in meter as well as the number of different bits after the location binarisation was performed. It can be seen that measurements one to eight are all within the accepted maximum distance between the GPS- and tower-based localisation of 320m. These locations differences result in less than 10 bits difference in the binary representation, which will be successfully corrected by the applied ECC. Therefore, the proposed verification algorithm will accept these location claims for the client to be genuine. In contrast, the last two measurements are outside this acceptable distance and result in 14 (respectively 48) bits difference in the binary representation. Therefore they will not be accepted by the verification algorithm.

B. Results

The experiments and trials were performed using four authentication factors, namely: F1 – Biometrics (Face biometric), F2 - a PIN for Shuffling & Transformation keys, F3 - Location, and F4 - Time.

Table II summarises the scheme performance based on the following 10 common scenarios evaluated in the experiments:

1) Biometric only: using face biometric without any other authentication factors and without UBRP.
2) All secure: using the four authentication factors under the assumption that all of them are secure.

TABLE I. LOCATION DATASET

	GPS-based Location (Loc_{GPS})		Tower-based Location (Loc_{Tower})		Distance: Loc_{GPS}, Loc_{Tower}	
	Latitude	**Longitude**	**Latitude**	**Longitude**	**Meter**	**Bits**
1	51.49772936	0.00761747	51.49700	0.00700	91.67	2
2	51.49890844	-0.05129457	51.49900	-0.05000	90.19	2
3	51.51427031	-0.14863729	51.51400	-0.14700	117.22	4
4	51.51405503	-0.14424384	51.51200	-0.14700	297.65	9
5	51.51317060	-0.14198542	51.51200	-0.13900	244.18	8
6	51.51053667	-0.14268279	51.51000	-0.14200	76.12	3
7	51.51385503	-0.14702438	51.51200	-0.14699	206.28	5
8	51.51377060	-0.14008542	51.51200	-0.13900	210.72	6
9	51.50422107	0.00083685	51.50800	-0.00200	463.81	14
10	51.50201261	-0.00130355	51.49800	-0.02400	1633.19	48

TABLE II. THE PERFORMANCE OF THE PROPOSED SCHEME IN DIFFERENT SCENARIOS

		Subset 1		Subset 2		Subset 3		Subset 4		Subset 5	
Simulating scenario		**FAR (%)**	**FRR (%)**	**FAR (%)**	**FRR (%)**	**FAR (%)**	**FRR (%)**	**FAR (%)**	**FRR (%)**	**FAR (%)**	**FRR (%)**
1	Biometric only	0	0	0.04	0.04	0.56	0.56	6.06	6.06	4.53	4.53
2	All secure	0	5	0	5.03	0	5.53	0	10.75	0	9.30
3	F1 compromised	0	5	0	5.03	0	5.53	0	10.75	0	9.30
4	F2 compromised	0	5	0	5.03	0	5.53	0	10.75	0	9.30
5	F3 compromised	0	5	0	5.03	0	5.53	0	10.75	0	9.30
6	F4 compromised	0	5	0	5.03	0	5.53	0	10.75	0	9.30
7	F2 & F3 compromised	0	5	0	5.03	0	5.53	0	10.75	0	9.30
8	F3 & F4 compromised	0	5	0	5.03	0	5.53	0	10.75	0	9.30
9	F2, F3, F4 compromised	0	0	0.038	5.03	0.53	5.53	5.76	10.75	4.30	9.30
10	All compromised	95	5	94.97	5.03	94.47	5.53	89.25	10.75	90.7	9.30

3) F1 compromised: simulating the scenario when facial feature vectors (i.e. the biometric authentication factor) are compromised.
4) F2 compromised: simulating the scenario when shuffling and transformation keys are compromised.
5) F3 compromised: simulating the scenario when location is compromised. This could happen when an imposter is physically close enough to the genuine client. This problem can be solved by a real-time message/call from the MNO to the mobile-handset asking for the client's permission before supplying the authenticator with the client's location. For example, a message such as "Authenticator XXX is requesting your location; would you like to proceed?"

In the case of a fake authentication attempt, the client stops the process. This solution does not work if the client's mobile-handset is stolen. However, the operator prompting the client/imposter for a password/PIN will resolve this. Of course, it can be argued that a password/PIN can equally be guessed. Therefore, there is a need to further simulate/investigate this scenario in the experiments.

6) F4 compromised: simulating the scenario when the transaction timestamp is compromised.
7) F2, F3 compromised: simulating the scenario when shuffling/transformation keys and location are compromised.
8) F2, F3 compromised: simulating the scenario when both timestamp and location are compromised.
9) F2, F3, F4 compromised: all authentication factors apart from the face biometric are compromised.
10) All compromised: simulating the scenario when an impostor has access to all four authentication factors e.g. using a malware on the mobile-handset.

Table II discloses the following observations. In scenario 1, face biometric only with the use of DWT Haar LH_3 as an efficient feature extraction tool has been simulated. The operating point (decision threshold) for each subset is selected at the Equal Error Rate (EER), i.e. FAR=FRR. From scenario 2 to 9, it can be seen that the proposed system is very secure (0% FARs) against any imposter attempt using facial images of different qualities (subset 1 to 5) even when one or more authentication factors are compromised. It is important to mention that although the scheme achieves the same FARs and FRRs in all scenarios from 2 to 9, this does not mean that the scenarios have the same level of security. Imposters in scenario 2 "All secure," for example, need to guess/fake four authentication factors whereas they only need to

guess/fake two authentication factors in scenario 9. This means that scenario 2 is much more secure compared to the scenario 9 even when the scheme achieves the same FARs and FRRs. This also illustrates the fact that FARs and FRRs are not sufficient to represent the security of such systems. Other factors such as the robustness against attacks (e.g. replay attack) and the level of difficulty needed to guess/fake each of the authentication factors should be taken into consideration.

In scenario 10, which can be seen as the most serious scenario all authentication factors are compromised. This can happen for example, when malware is installed on the mobile-handset, which is able to capture all authentication factors individually and send it to a remote adversary. Assuming that the adversary knows the underlying algorithm's details, the adversary can produce a "fresh" mFactor and submit it to the authenticator claiming to be a genuine client. Even in such scenarios, the proposed scheme might offer the authenticator two lines of defence, namely the location of the registered mobile-handset that will be checked by the second independent source, and biometric features that need to be different every time (no two biometric samples are exactly the same). However, if the adversary is at the same time a) clever enough to change the biometric feature vector slightly in his offensive attempt, b) lucky enough to be physically close enough to the client's mobile handset (within 320m) or c) knew the current whereabouts of the legitimate client's mobile-handset, our proposed scheme would have been undermined. However, it is important to stress here that the contribution of this paper is the proposed combination of the different authentication factors that offers additional security over previously proposed systems. This paper does not claim that the proposed system can withstand all possible attack scenarios as no system should claim. However, we strongly believe that this proposal makes it more difficult for an adversary and that the proposal offers stronger security compared to previously proposed schemes.

V. Conclusion

In this paper, an effective, practical scheme for unattended and remote authentication from mobile-handsets by incorporating cancellable biometrics with actual mobile-handset location and real-time to produce a one-time authentication token is proposed. For added security, the location is obtained via two independent sources, and the authentication token is robustly stamped by the transaction time to grantee the liveliness.

It can be argued that the proposed scheme is robust against replay attack due to the fact that replaying an intercepted mFactor is very difficult to fool the authenticator for two reasons: a) the timestamp expiry and b) the location verification at the authenticator side.

Furthermore, the complex combination of the four authentication factors to produce the mFactor makes the transmitted mFactor leak no information about the employed authentication factors, which eliminates the risk that an adversary can learn useful information from previously intercepted mFactor transmissions.

References

[1] S. Z. Li and A. K. Jain, *Encyclopedia of Biometrics*, Springer, U.S.A, 2009.

[2] K. Nandakumar, "Multibiometric systems: Fusion strategies and template security," Ph.D. dissertation, Michigan State Univ., Michigan, MI, 2008.

[3] S. Jassim, H. Al-Assam, and H. Sellahewa, "Improving performance and security of biometrics using efficient and stable random projection techniques," in *Proc. 6th International Symposium on Image and Signal Processing and Analysis*, 2009, pp. 556 - 561.

[4] A. T. B. Jin, D. N. C. Ling, and A. Goh, "BioHashing: Two factor authentication featuring fingerprint data and tokenised random number," *Elsevier Pattern Recognition*, 2004, pp. 2245-2255.

[5] T. Kuseler and I. A. Lami, "Using geographical location as an authentication factor to enhance mcommerce applications on smartphones," *International Journal of Computer Science and Security*, vol. 6, 2012, pp. 277-287

[6] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in *Proc. 2nd ACM Workshop on Wireless Security*, 2003, pp. 1–10.

[7] I. A. Lami, T. Kuseler, H. Al-Assam, and S. A. Jassim, "Locbiometrics: Mobile phone based multifactor biometric authentication with time and location assurance," in *Proc. 18th Telecommunications Forum*, 2010.

[8] H. Al-Assam, H. Sellahewa, and S. A. Jassim, "A lightweight approach for biometric template protection," in *Proc. SPIE*, 2009, pp. 73510.

[9] H. Al-Assam and S. A. Jassim, "Security evaluation of biometric keys," *Journal of Computers & Security*, vol. 31, no. 2, pp. 151-16, 2012.

[10] S. Cox, *An introduction to LTE: LTE, LTE-advanced, SAE and 4G mobile Communications*, John Wiley & Sons, ch. 17, 2012, pp. 270-270.

[11] T. Kuseler, H. Al-Assam, S. Jassim, and I. A. Lami, "Privacy preserving, real-time and location secured biometrics for mCommerce authentication," in *Proc. SPIE Mobile Multimedia/Image Processing, Security, and Applications*, 2011, pp. 80630G.

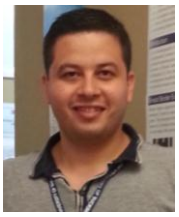
[12] U.S. Federal Communications Commission, Public Safety and Homeland Security Bureau, 9-1-1 Service, [Online]. Available: http://transition.fcc.gov/pshs/services/911-services/

[13] H. Al-Assam, H. Sellahewa, and S. A. Jassim, "Secure wavelet-based isometric projection for face recognition," in *Proc. SPIE Mobile Multimedia/Image Processing, Security, and Applications*, 2011, pp. 80630U.

[14] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Transactions on Computers*, vol. 55, no. 9, pp. 1081-1088, September 2006.

[15] A. S. Georghiades, P. N. Belhumeur, and D. J. Kriegman, "From few to many: Generative models for recognition under variable pose and illumination," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 23, no. 6, pp. 643–660, 2001.

[16] Followus–mobile Phone Tracking Specialists. [Online]. Available: http://www.followus.co.uk/



Hisham Al-Assam, BEng, DPhil
Hisham is a post-doctoral research assistant at the applied computing department, the University of Buckingham, UK.
His main expertise is in biometric template security and user privacy, multi-factor and multi-modality authentication, remote biometric authentication for mobile transactions, cancellable biometrics, biometric-based cryptographic key generation and security analysis. His recent research interests also include biomedical image processing and analysis, and applied compressive sensing.

Ihsan A. Lami, DPhil
Ihsan is a Reader in Computer Science at the School of Science, Medicine and Dentistry at the University of Buckingham, UK.
His research teams focus on Smartphone based applications for localisation, Cloud Computing Services and Networking.

Torben Kuseler, Diplom Computer Science (FH), M.Sc., DPhil
Torben holds a Diplom in Business Information Technology (FH Wedel, Germany), an MSc (FH Wedel, Germany) and a PhD in Computer Science (University of Buckingham, UK).
He is currently a post-doctoral research associate with the Applied Computing Department at the University of Buckingham, UK. His research activities are focus on Authentication on mobile devices, Localisation techniques and location-based services (LBS) as well as Software protection and Software security.