Cryptography Based Authentication Methods

Mohammad A. Alia, Abdelfatah Aref Tamimi, and Omaima N. A. AL-Allaf

***Abstract*—This paper reviews a comparison study on the most common used authentication methods. Some of these methods are actually based on cryptography. In this study, we show the main cryptographic services. As well as, this study presents a specific discussion about authentication service. Since the authentication service is classified into several categorizes according to their methods. However, this study gives more about the real life example for each of the authentication methods. It talks about the simplest authentication methods as well about the available biometric authentication methods such as voice, iris, fingerprint, and face authentication.**

***Index Terms*— Keywords: information security, cryptography, system access control, authentication, and network security.**

I. INTRODUCTION

INFORMATION security is the process which describes all measures taken to prevent unauthorized use of electronic data, whether this unauthorized use takes the form of destruction, use, disclosure, modification, or disruption. Information security and cryptography are interconnected and share the common services of protecting the confidentiality, integrity and availability of the information ignoring data form (electronic document, printed document). In the encryption process, information security uses cryptograph to shift the information into the cipher form which does not allow it to be used by unauthorized personnel.

Cryptography provides the information security for other useful applications such as in encryption, message digests, and digital signatures. The length and strength of the Cryptography keys are considered an important mechanism. The keys used for encryption and decryption must be strong enough to produce strong encryption. They must be protected from unauthorized users and must be available when they are needed. Cryptography also contributes to computer science, particularly, in the techniques used in computer and network security for access control and information confidentiality. Cryptography is also used in many applications encountered in everyday life such as: computer passwords, ATM cards, and electronic commerce (refer to Figure 1). The request for Cryptography system has increased recently for the public especially after the fast development of the Internet in the last 10 years ago.

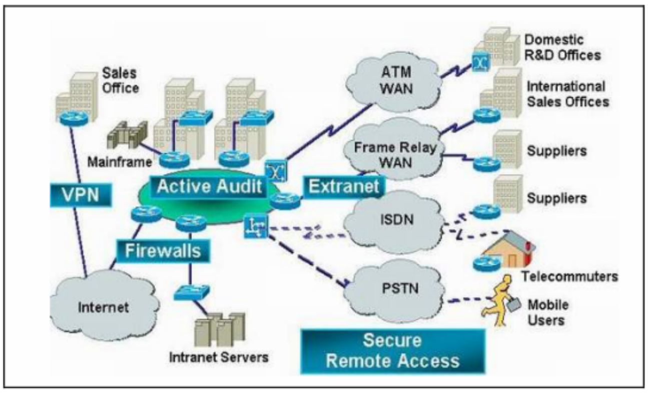


Figure 1: Network security system [1]

This paper summarized the development in cryptography based authentication. The paper discusses the latest development on the real life authentication methods which include symmetric, public-key, token, and biometric authentication methods.

II. CRYPTOGRAPHY

Cryptography is one of the most important fields in computer security. It is a method of transferring private information and data through open network communication, so only the receiver who has the secret key can read the encrypted messages which might be documents, phone conversations, images or other form of data (refer to Figure 2).

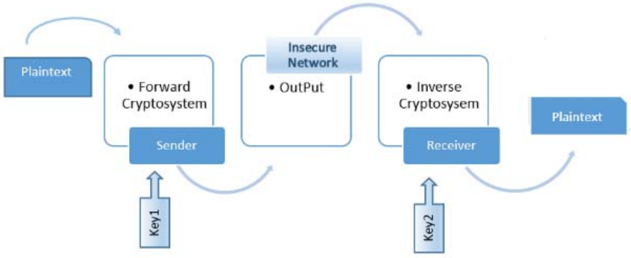


Figure 2: Cryptography scheme

To implement privacy simply by encrypting the information intended to remain secret can be achieved by using methods of Cryptography. The information must be scrambled, so that other users will not be able to access the actual information. For example, in a multi-users system, each user may keep his privacy intact via her/his own password. On internet, a large number of internet users use

Manuscript received June 10, 2014; revised July 09, 2014. This work was supported in part by Al Zaytoonah University of Jordan.

All authors are with Faculty of Science and Information Technology – Al Zaytoonah University of Jordan, P.O.Box: 130 Amman (11733) Jordan.
Email of Dr. Mohammad A. Alia is dr.m.alia@zuj.edu.jo.
Email of Dr. Abdelfatah Aref Tamimi is drtamimi@zuj.edu.jo.
Email of Dr. Omaima N. A. AL-Allaf is omaimaalallaf@zuj.edu.jo

internet application, such as business, research, learning, etc. These activities are very important for the users' application; hence, the importance of using Cryptography has been highlighted to help them keep the privacy.

Cryptography services in general help to ensure the following [3]:

- Authentication: Authentication is a service used to provide the identity of an entity.
- Confidentiality: Confidentiality is a service used to guarantee information it is accessible only to authorized entities and is inaccessible to others.
- Integrity: Integrity is a service used to guarantee that the information remains unchanged from the source entity to the destination entity.
- Non-repudiation: Non-repudiation is a service used to confirm the involvement of an entity in a certain form communication, and prevents any party from denying the sent message.
- Accessibility: Accessibility is a service put in place to allow the use of information resources by authorized entities.

Cryptography algorithms can be classified into three board categories, asymmetric (public-key) cryptosystem, symmetric (secret-key) cryptosystem and hash functions (refer to Figure 3). In general, Cryptography protocol employs asymmetric cryptosystem to exchange the secret key and then uses faster secret key algorithms to ensure confidentiality of the data stream [2, 3]. Symmetric cryptosystem (Secret-key algorithm) is used to encrypt and decrypt messages by using the same secret key. While hash functions are a non-public key cryptography and work without key. As well hash functions are normally used as data integrity primitive in more complicated cryptographic protocols. However, the secure hash algorithm (SHA) was issued by the National Institute of Standards and Technology in 1995 as a FIPS [4]. Asymmetric cryptosystem on the other hand, works in a very different way. In public key algorithm, there are two keys; both belong to one party, either the recipient or the sender. One key is used to accomplish half of the task (e.g. encryption) while the other key will be used to complete the rest of the task (e.g. decryption).

III. System Access Control (Logging to System)

The system access control process [5] is interconnected and shared between the information security and cryptographic aspects. Ensuring that unauthorized users don't get into the system. The system control also protects password data and keeps track of who's doing what in the system. However, this process is used to ensure that the system it is accessible only to authorized entities and is inaccessible to others. System access control process provides the computer security with the first security layer by controlling access to that system: Who's allowed to log in? How does the system decide whether a user is legitimate? How does the system keep track of who's doing what in the system?

However, logging into a system by the access control process is a kind of challenge/response scenario. This scenario should be done by identification and authentication processes.

Identification and authentication [5] (I&A) is the process that can be used to identify and verify the users on their secure systems. In secure system, the user must identify himself/herself, then the system will authenticate the identity before using the system. However, authentication verifies the user who is requesting access process of determining the identity of a user that is attempting to access a system [5, 7]. Therefore, the identification and authentication processes can be done successfully through the following three classical ways:

1. Something known: password, or a personal identification number (PIN).
2. Something possessed: smart card or token.
3. Something inherent: face (Biometric) detection and recognition, fingerprint, voice, retina, or iris characteristics.

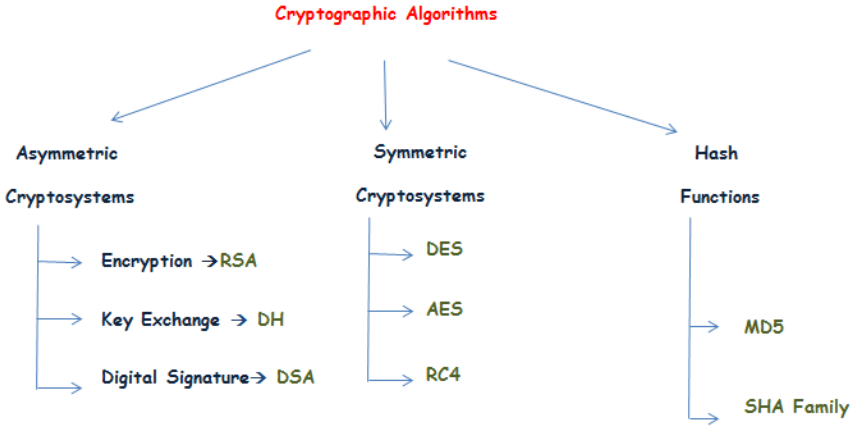


Figure 3: Main branches of Cryptography

On other hand, the identification and authentication processed can be also professionally seen as:

4. SMS based authentication
5. Symmetric-key authentication
6. Public-key authentication

Meanwhile, this study discusses the common used authentication techniques on our lifetime. As well as, it shows a performance comparison study between them in tem of the security level and the execution time.

IV. Authentication Methods

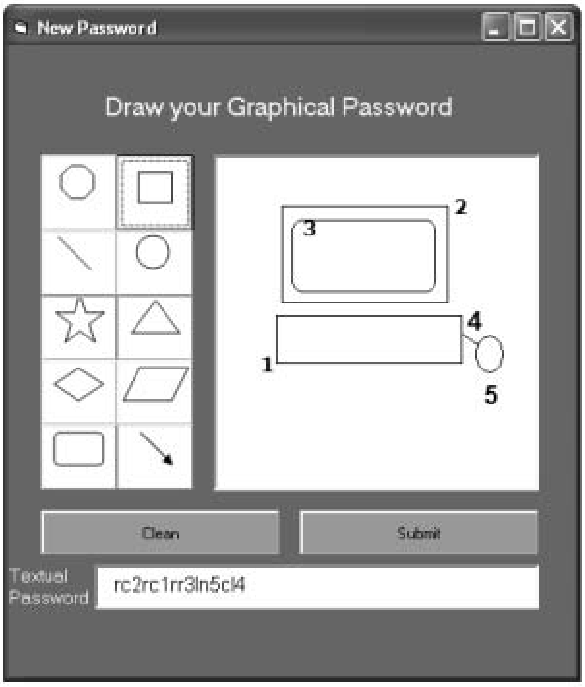
A. Password authentication protocol

A password authentication protocol (PAP) is an authentication protocol used by Point to Point Protocol to authenticate users before allowing them access to data resources. Password [6] is the most common used method in authentication protocols. Whereby, the user should prove his/her username and password by comparing it with the system stored value. This authentication method is important for users since it is easy to be memorized. However, password can be recently classified into two main types; textual password and graphical password.

Graphical password: A graphical password (refer to Figure 4) is one of the most important fields of authentication in system access control techniques. It allows users to draw or select their passwords from images bar, in a specific order. Then the password will be presented in a graphical user interface (GUI). On other hand, the graphical password is also defined as graphical user authentication (GUA). Therefore, graphical password is considered easier than other password techniques base text, since it is easy to be remembered for most computer users. In term of security, graphical password offers better security than other textual passwords because the graphical password is created by selectable images as a series. These series is normally combined in specific order of images. Therefore, the graphical passwords are recently designed to be resisted to many kinds of attacks such as; shoulder-surfing. Whereas, it will be difficult to recognize the exact images series order (graphical password) by attackers [7].

B. Authentication Token

Is a portable device used for authenticating users (refer to figures 5, 6, 7, and 8), thereby it is allowing authorized access into a network system. Authentication technique using a portable device to carry the embedded software that is called software token. There are several token systems, among these are: RSA SecureID Token Cryptocards, Challenge Response Token, and Time based Tokens. However, Challenge Response Token is an authentication technique using a calculator type token that contains identical security keys or algorithms as a Network Access Server (NAS) [8].



New Password

Draw your Graphical Password

Textual Password: rc2rc1rr3ln5cl4

Figure 4: Graphical password [7]

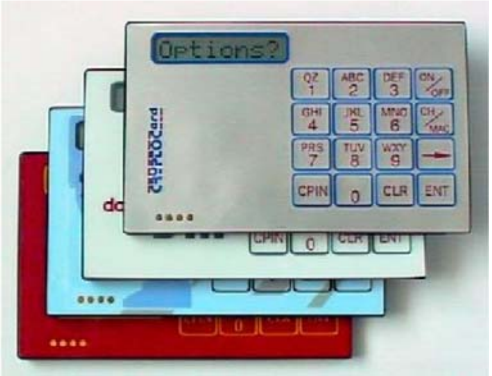
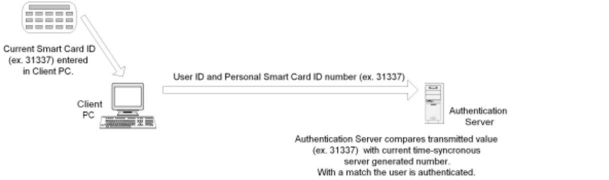
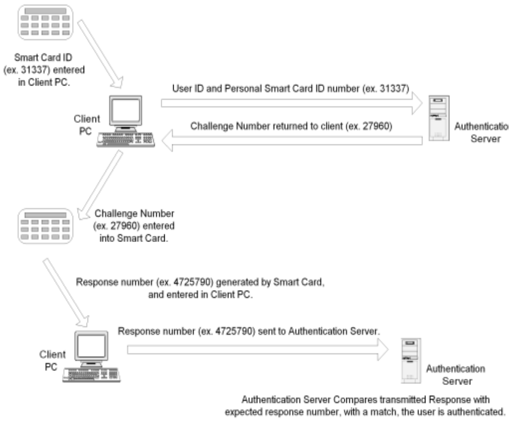


Figure 5: the challenge response card from Cryptocard [8]



Current Smart Card ID (ex. 31337) entered in Client PC.
User ID and Personal Smart Card ID number (ex. 31337)
Client PC
Authentication Server
Authentication Server compares transmitted value (ex. 31337) with current time-syncronous server generated number. With a match the user is authenticated.

Figure 6: An example of the Time-based Token Authentication System [8].



Smart Card ID (ex. 31337) entered in Client PC.
User ID and Personal Smart Card ID number (ex. 31337)
Client PC
Challenge Number returned to client (ex. 27960)
Authentication Server
Challenge Number (ex. 27960) entered into Smart Card.
Response number (ex. 4725790) generated by Smart Card, and entered in Client PC.
Response number (ex. 4725790) sent to Authentication Server.
Client PC
Authentication Server
Authentication Server Compares transmitted Response with expected response number, with a match, the user is authenticated.

Figure 7: Token Authentication System [8].

Figure 8: RSA SecureID Token [8]

C. Symmetric-key Authentication

In symmetric key authentication, the user shares a single, secret key with an authentication server (normally the key is embedded in a token) [9]. The user is authenticated by sending to the authentication server his/her username together with a randomly challenge message that is encrypted by the secret key. Whereby, the user is considered as authenticated user if the server can match the received encrypted message using its share secret key.

D. Public key authentication: Diffie-Hellman Authentication

The key exchange is an important method in public-key Cryptography for providing authentication cryptographic service. It was the first public-key cryptographic scenario as developed by Whitfield Diffie and Martin Hellman [10], were the first who developed the key exchange algorithm that is called DH. In DH, keys are exchanged between the users according to Cryptography protocols which are based on the key exchange problem. They highlighted the most important method of exchanging the keys by using the discrete logarithm hard problem (refer to Figure 9).

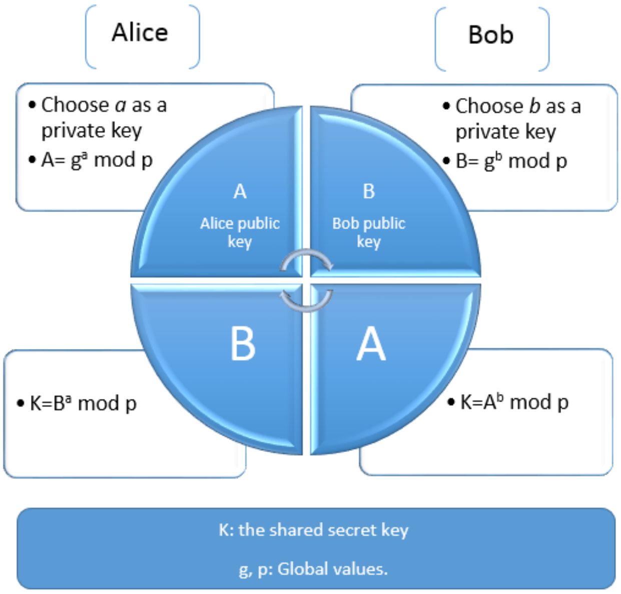


Figure 9: Diffie-Hellman key exchange protocol

E. Biometric authentication

A biometric authentication is a digitizing measurements of a physiological or behavioral characteristic for human. A biometric authentication systems can theoretically be used to distinguish one person from. However, many biometric authentication systems have been proposed which are categorized as; face detection authentication system, fingerprint authentication system, Iris authentication system, and voice authentication system [11] (refer to Table 1).

1) Fingerprint recognition

A fingerprint system uses an electronic device to capture a digital image of the fingerprint pattern. This captured image in fingerprint system is called a live scan which is digitally processed to create a biometric template (finger features). The biometric features will be later stored and used for matching process.

2) Voice biometric authentication

Voice biometric authentication is the use of the voice pattern to recognize the identity of the person. Meanwhile, voice authentication is now considered as a fast wide deployed form of biometric authentication. However, it is one of the best methods of determining the biometric method efficacy. However, voice recognition is categorized into five types: speaker dependent system, speaker independent system, discrete speech recognition, continuous speech recognition, and natural language.

3) Face detection

Face detection and recognition systems are a two complementary scenarios [11]. Face detection is as technology uses learning algorithms to allocate human faces in digital images. As shown by Figure 10, face detection algorithm focuses and determines the facial features and ignores anything else in the digital images [11, 12]. Moreover, many face detection techniques have been presented such as; Viola and Jones face detection [13], face detection based Adaboost [14], semi-supervised learning for facial expression recognition [15], and etc.

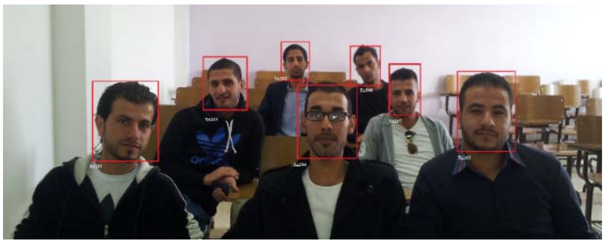


Figure 10: Face detection [11].

Furthermore, face recognition technology is a natural biological authentication process according to the cognitive rule of human beings. This technology is used to identify any given face image using the main features of this face [16]. Normally, face recognition process works after face detection process to identify the detected face by comparing the detected faces with the stored faces images. In general, different artificial neural network algorithms have been proposed such as; feed forward back propagation neural network (FFBPNN), cascade forward back propagation neural network (CFBPNN), function fitting neural network (FitNet), and pattern recognition neural network (PatternNet) algorithms [16]. Since, Soon and Seiichi [17], While Volkan [18], Weihua and WeiFu [19] are recognition systems applied on neural algorithms.

4) Iris Authentication

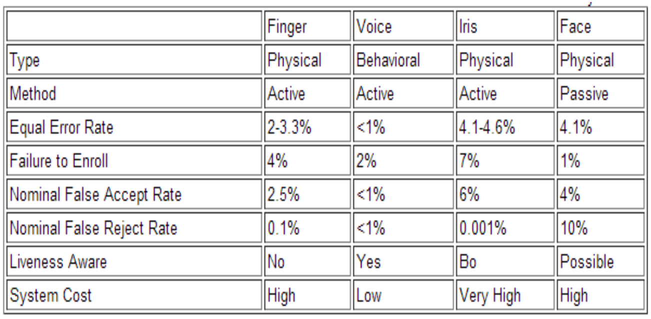
Actually, iris and fingerprints are parallel in their uniqueness technology. Worldly, the statistical result of the iris usage in authentication is presents that iris is one of the best ways of meeting high risk situations. Iris recognition software is currently in wide use at airport borders. As well as, it is also widely used at many other industries for doing authentication.

V.DISCUSSION

As discussed earlier, password authentication system is the most common used method in authentication protocols. In the meantime, password works with very low cos, since it just needs keyboard system or mouse system in best cases. In term of security, the use of password authentication is considered very weak, this is because of the software attacks. However, password software attack is embedded and activated by visiting a fake site that looks like the normal commercial site (phishing attack). As well as, some fake web site has developed keyboard logging software to copy the user ID and password. On other hand, this study shows that the password authentication system is highly secure if the password is computed between the communication parties over insecure medium by using public-key cryptographic system such as DH protocol. However, the comparison talks about the security token which is more closely with the users. It reduces the risk on the user password, since the password can be sometime encrypted by the embedded public key cryptosystem. Moreover, the standard token system is only useful for low to medium risk type authentication situations. Whereby, High risk authentications should implement multi-factor authentication.

In biometric systems, iris biometric authentication should be provided for high risk conditions. Whereby, voice authentication is efficiently the fast wide deployed form of biometric authentication. As well as, face recognition algorisms are considered more complex and secure than other authentication algorithms such as fingerprint, iris and voice authentication algorithms. Comparing face recognition to other techniques, face recognition is featured as: accurate and fast Identification, and high usability and security (refer to Table 1).

TABLE 1:
PERFORMANCE COMPARISON BETWEEN BIOMETRIC AUTHENTICATION METHODS [20]



	Finger	Voice	Iris	Face
Type	Physical	Behavioral	Physical	Physical
Method	Active	Active	Active	Passive
Equal Error Rate	2-3.3%	<1%	4.1-4.6%	4.1%
Failure to Enroll	4%	2%	7%	1%
Nominal False Accept Rate	2.5%	<1%	6%	4%
Nominal False Reject Rate	0.1%	<1%	0.001%	10%
Liveness Aware	No	Yes	Bo	Possible
System Cost	High	Low	Very High	High

VI. CONCLUSION

This paper summarizes the difference between cryptography based authentication methods. It shows the possibility of using public key cryptosystem to provide high level of authentication security. The surveyed methods are password, public key sharing, symmetric key, token, and biometric authentication methods. The performance of these methods are actually different according to their tools cost, execution time and the security. However, this study highlights that the DH public key method provides high level of security to distribute the secret key (password) between users over insecure communication without any extra tool cost. Whereby, most of the biometric methods are also secure, professional and provides very accurate authentication process, but sometime they need extra tools which are required extra cost. Therefore, the surveyed public key authentication is good alternative to the traditional biometric methods.

ACKNOWLEDGMENT

The authors would like to thank Al Zaytoonah University of Jordan for supporting this study.

REFERENCES

[1] Macroview Telecom Group (2006) Network Security Solutions. Macroview Telecom Group. Available from World Wide Web: www.macroview.com/solutions/infosecurity/
[2] Branovic, R. Giorgi, E. Martinelli, “Memory Performance of Public-Key Cryptography Methods in Mobile Environments”, *ACM SIGARCH Workshop on Memory performance: Dealing with Applications, systems and architecture (MEDEA-03)*, New Orleans, LA, USA, pp. 24-31, 2003.
[3] Menezes, A., P. Van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, pp.4-15, 516, 1996.
[4] NIST, “Secure Hash Standard,” *Federal Information Processing Standard, FIPS-180-1*, 1995.
[5] R. Lehtinen, (2006), “Computer Security Basics”, 2nd Edition, O'Reilly, ISBN-10: 0-596-00669-1.
[6] W. Stallings, “Cryptography and Network Security Principles and Practices”, Pearson Education, 5rd edition, 2011.
[7] M. Alia, A. Hnaif, H. Al-Anie, and A. Tamimi. "Graphical Password Based On Standard Shapes", *Science Series Data Report* ,Vol 4, No. 2;Feb 2012
[8] Cisco. Security Certified Program – SCP. 2007.

[9] Government Chief Information Officer. "e-Authntication". http://www.e- authentication.gov.hk/en/professional/skey.htm, 2014.

[10] W. Diffie, and M. E. Hellman, “New Directions in Cryptography”, *IEEE Transactions on Information Theory*, IT-22, pp. 644-654, 1976.

[11] M. Alia A. Tamimi O. AL-Allaf. "Integrated System For Monitoring And Recognizing Students During Class Session". The *International Journal of Multimedia & Its Applications (IJMA)*, Vol.5, No.6. 2013.

[12] I. Marqu´es, and M. Gra˜na. Face Recognition Algorithms. Proyectos Fin de Carrera, Universidad Carlos III de Madrid.2010.

[13] P. Viola , and M. Jones.Rapid object detection using a boosted cascade of simple features. *Accepted Conference On Computer Vision And Pattern Recognition*, 2001.

[14] Yan-Wen Wu , and Xue-Yi Ai. Face Detection in Color Images Using AdaBoost Algorithm Based on Skin Color Information. *First International Workshop on Knowledge Discovery and Data Mining*, 2008.

[15] I. Cohen , N. Sebe , F. G. Cozman ,Thomas S. Huang . Semi-Supervised Learning for Facial Expression Recognition. *Proceedings of the 5th ACM SIGMM international workshop on Multimedia information retrieval.* ACM New York, NY, USA Pages 17 – 22.

[16] O. N. A. AL-Allaf, A. Aref Tamimi , and M. A. Alia. Face Recognition System Based on Different Artificial Neural Networks Models and Training Algorithms. *International Journal of Advanced Computer Science and Applications,* Vol. 4, No. 6, 2013.

[17] S. L.Toh and O. Seiichi. A Face Recognition System Using Neural Networks with Incremental Learning Ability. *Proceeding of the 8th Australian and New Zealand Conf. on Intelligent Information Systems.* pp.389-394. 2003.

[18] A. Volkan . Face Recognition Using Eigenfaces and Neural Networks. Master of Science Thesis, The Graduate School of Natural And Applied Sciences. The Middle East Technical University. 2003.

[19] W. Weihua and W. WeiFu . A Gray-Scale Face Recognition Approach. Second International Symposium on Intelligent Information Technology Application, 978-0-7695-3497-8/08, *IEEE computer society.* 2008. DOI= 10.1109/IITA.2008.101.

[20] G. Huntington. "AuthenticationWorld.Com- The business of authentication". Available: http://www.authenticationworld.com/Authentication-Biometrics/