Journal of Engineering Sciences
Vol 12, Issue 06, JUNE /2021
ISSN NO:0377-9254

SECURE BANK AUTHENTICATION USING IMAGE STEGANOGRAPHY BASED ENCRYPTION

[1]***K.Naveen,*** [2]***Dr. R Tamilkodi ,*** [3]***Mr. K Praveen Kumar***
[1]***PG student,*** *Department of Computer Applications, Godavari Institute of Engineering And Technology(Autonomous),Rajahmundry, AP*
[2]***Professor,*** *Department of Computer Applications, Godavari Institute of Engineering And Technology (Autonomous), Rajahmundry, AP*
[3]***Assistant professor,*** *Department of Computer Applications, Godavari Institute of Engineering And Technology(Autonomous), Rajahmundry, AP*
Email: *[1]naveenkundeti7799 @gmail.com, [2]hod.mca@giet.ac.in, [3]praveenkumar@giet.ac.in*

Abstract

Arising new Technologies and enormous scope organizations have made this world, a worldwide town. Numerous business associations offer online types of assistance focusing on worldwide customer bases. Exchange in worldwide scale has been empowered by banks from one side of the planet to the other through E-banking to supply the necessities of above business associations. E-banking serves loads of advantages to the two clients of banks and banks itself. It increases the value of consumer loyalty's with better help quality and empowers banks to acquire an upper hand over different contenders. Internet banking need to have undeniable level security to give protected, reliable, and vigorous online climate which ensures secure information transmission and character of both bank and client. Absence of safety may prompt less trust or difficult to confide in mentality towards internet banking. Despite the fact that clients are pulled in by internet banking comfort, they appear to be to a great extent in worry about data fraud and phishing .Investigation of many exploration papers on e-banking security models and their particular benefits and disservices have been examined in writing audit. Username, secret key, E-banking dongles, fractal pictures, biometric checks and progressed encryption principles are a portion of the recommended answers for E-banking security. This investigation centers around the security past above systems. This paper guarantees security of web based banking at three levels. At customer side, utilizing web dongle coordinated with finger impression filtering innovation, at banking cut off side and information transmission level. This model likewise incorporates username, secret key and progressed encryption for additional security. Complete depiction on the model has been talked about in approach segment. Future chips away at this subject and Conclusion are shrouded in independent areas.

Index Terms: E-banking, Phishing, Fractal image, Biometric Scans, Encryption, Finger Prints, Server Side.

1.INTRODUCTION

Data Technology and Internet Networks have shown a huge advancement over past many years, which prompted viable Electronic Commerce (E-business) exercises at worldwide level. Significant objectives of E-trade are fast and adaptable data trade and improved client administrations to acquire[1] more trust. Banking industry give[2] E-trade administrations through Electronic banking[3] or internet banking. Internet banking offers esteem added[4] administrations and comfort to its clients. It likewise permits clients to make monetary exchanges through the site of particular bank[5]. Opening financial balances, giving charge cards, paying and getting credits and obligations, working with web based[6] shopping and online bill instalments through ledgers are most regular administrations [7]offered by web based financial destinations. All in all these frameworks empower clients to get to their record[8], acquire data

on the monetary items, move cash and use different contributions of banks[9]. Internet banking gives innumerable benefits to both financial industry and its clients. It empowers the clients to make enormous exchanges worth a few millions or straightforward exchanges worth few rupees in matter of seconds without visiting the bank genuinely[9]. Along these lines clients have no compelling reason to stand by in long lines to recover bank administrations. Web based banking is straightforward entry and time serving. From banks viewpoint, saving can be produced using lessening staff compensation, branch office, and Automatic Teller Machine (ATM) and Electronic Funds Transfer at Point[10] of Sale(EFTPOS) exchange support financial plans[11]. Furnishing banking administrations with the important security from a distant area through the web [12]is a difficult cycle in financial area. Likelihood of assaults increment with the headway of internet banking administrations[13]. Billions of monetary information exchange [14]is directed online consistently. Hence not accomplishing a view of safety will have the more extensive impact of diminishing clients'[15] trust in web banking just as the bank.

Talented criminal programmers' carryout bank digital wrongdoing [16]assaults ordinarily by controlling the banks' online data framework. Guaranteeing ideal security in web based [17]banking is difficult to accomplish focus with judicious customer Personal Computer (PCs)[18], which are not intended for secure web business exchange. Numerous explores have announced that criminal [19]assaults on web banking have gotten more mind boggling, especially with the improvement of key lumberjack programming. Man-in the center assaults is basic assault of above kind[20]. This raises a solid contention about the adequacy of the framework that depend on confiding in the customer. Thusly, there is a need to guarantee customer, banking worker and the way from customer to banking cut off are appropriately gotten with security calculations. Current web banking models center around distinguishing proof as opposed to extortion avoidance. Thus, there is a need to build up a reasonable framework for E-banking security which empowers required security and tackles the defects recognized in the current web banking framework. This exploration work recommends an E-banking security model to tackle serious issues experienced in current web banking framework. This model comprises of E-banking dongle with unique mark scanner to guarantee genuine customer and progressed encryption system for monetary information transmission.

2.LITERATURE REVIEW

In the current decade E – banking is becoming tremendously ludicrous. Fakes in E-Banking exchange is serious everywhere on the world. There are numerous explores and studies proceeding to decrease E-Banking cheats and clear a path to a superior financial exchange to the buyers[21]. Hence, there are numerous specialized and hypothetical arrangements have been proposed in numerous district of the world. At the point when examination group [22]went through among the exploration papers the group discovered a few arrangements and thoughts as follows, Use of username and secret phrase[23] is a typical and customary way that assists with shielding each exchange from the financial cheats just as programmers. At the point when a purchaser needs to make an exchange, he/she ought to check his/her personality with the utilization of username and secret word[24]. Specialist Hameed U Khan has proposed a method which will augment the security level of the exchange. The exploration paper contains that utilization of Secret picture/Iris example will upgrade the security level of the E – Banking exchange. It incorporates one-time passwords to check[25] the buyer whether he/she is the right individual or not. The client should enter the one-time secret word message and send it back to the worker to start the exchange. Exploration asserts another procedure called [26]Three-level Security Implementation to give a protected and solid E-Banking arrangement. The Three-level Security

Implementation contains 3 fundamental regions like security module, network module and control module. The security module incorporates another 3 sorts of independent modules, for example, client validation module which will incorporate a bio metric output (Finger Print) and security pin check to associate with the financial worker. These subtleties of the shopper will be scrambled and ship[27] off the Kerberos worker. Purchaser should utilize a different dongle to speak with the financial worker. When the subtleties of the shopper got the worker will check the scrambled subtleties and macintosh address of the e-banking dongle.

At the point when the check is effectively finished the Kerberos worker will permit the purchaser to speak with the financial worker with the utilization of Transaction information security module. K. Thamizhchelvi [28]and G. Geetha have concocted a thought called Message Authentication Image (MAI) Algorithm saying that it will be an extraordinary method to give a protected exchange. The methodology says that when the client enters his/her client name to begin an exchange the worker will produce and send a pass mark picture to the specific shopper[29]. Assuming that picture matches with the buyer's one, worker will permit the customer to enter his secret phrase. The buyer needs to send his fractal picture to the worker[30]. At the point when both fractal picture and secret word coordinates with the worker will permit the specific buyer to start the exchange. The pass mark picture is utilized to check that the buyer is correspondence with the right worker and the fractal picture is utilized to confirm that the worker is speaking with the right client. Kovach S.et.al shows an extortion identification framework proposed for internet banking that depends on neighborhood and worldwide conduct in this exploration paper. Extortion location contains in recognizing such informal movement once the misrepresentation counteraction has fizzled. Among the strategies utilized by fraudsters, ―phishing‖.

3.METHODOLOGY

The proposed framework comprises three principle stages to achieve E-banking security. They are, Client confirmation stage, Server check stage, Secured information transmission stage. Progressed Encryption components are utilized at every single periods of the proposed framework to guarantee progressed security. Public and private keys of Client, Authentication worker and Banking worker are utilized for this reason.

3.1 Client Verification Phase

Customer check stage is one of the significant stage in E-banking security as numerous cheats identified with E-banking occur due to impersonalized gatecrashers. This stage guarantees that, Original client is mentioning for E-banking administrations. This is carried out utilizing MAC address of banking dongle, Finger print data of specific client, private username and one-time secret key. Beginning solicitation for E-banking activity is send with the MAC address of E-banking dongle of specific client. Further tasks are completed just if the MAC address is substantial. Next the unique mark of the client is checked for approval. In the event that the outcome is positive, the framework prompts username. For accurately entered username, once secret word is given through SMS and customer confirmation measure reaches a conclusion.

3.2 Server Verification Phase

server confirmation stage guarantees that the customer is getting to a unique E-banking site. This is carried out by approving the unique mark at customers' end. Fingerprints of substantial clients are put

away in the information base of the financial worker. This unique mark data is ship off the legitimate customer demand. The E-banking dongle application permits further E-banking measure just if both the unique mark data matches with one another. This unique finger impression approval confirms innovation of the two players all at once (for example just the first financial site will actually want to send unique finger impression of unique customer).

3.3 Secured Data Transmission Phase

This stage guarantees that the E-banking administration tasks are done safely between customer's end and worker end. This is executed with the utilization of brief meeting keys for encryption and decoding of exchange data. Meeting keys are given toward the finish of customer and worker check measures. Meeting key is encoded with public key of customer and private key of E-banking worker and gave to the customer. Meeting key is encoded utilizing private key of E-banking worker to guarantee that the meeting key is given by unique E-banking site and scrambled utilizing public key of customer to guarantee that the meeting key is decoded exclusively by unique customer. Meeting keys get lapsed either, if no exchange is recorded inside 10 minutes of inception or if client demand meeting end.

3.4 New System Overall Process

The following section describes how the proposed online banking security model works. The process of connecting client to the server, transaction information exchange and connection termination are being explained in a step by step by manner below.

Step 1. Once the intended user inserts the banking dongle which has internet connectivity and finger print scanner technology, dongle automatically sends a request to the authentication server.

Step 2. Authentication server checks the MAC address of requesting dongle for client verification, if it is a valid client, Authentication server sends a request to Banking server for the finger print of particular user.

Step 3. Banking server sends the finger print of respective user, after encrypting it with Banking servers' private key and public key of Authentication server.

Step 4. This finger print is decrypted with suitable keys at Authentication servers' end, again encrypted with Authentication servers' private key and forwarded to Client.

Step 5. Preliminary server verification is conducted at clients' end by matching the received finger print with the users' finger print scanned at the movement of inserting dongle.

Step 6.If the result is positive, the dongle application prompts username of the user and sends the retrieved information to the authentication server after encrypting it with the public key of Authentication server.

Step 7.If the username is valid password text box is enabled and one-time password is send to the user through SMS.

Step 8.When authentication server confirms the identity, session key for further data transmission which is encrypted with private key of Authentication server and public key of respective user is send to the user.

Step 9.Both banking server and client device uses this session key to encrypt and decrypt transaction information.

Step 10.Session key get expired if there aren't any transactions observed within 10 minutes of session initiation.

Step 11.Once the user request to terminate the operation, session key get expired and dongle application get closed after notifying the user.

Step 12.User ejects the dongle from their client device.

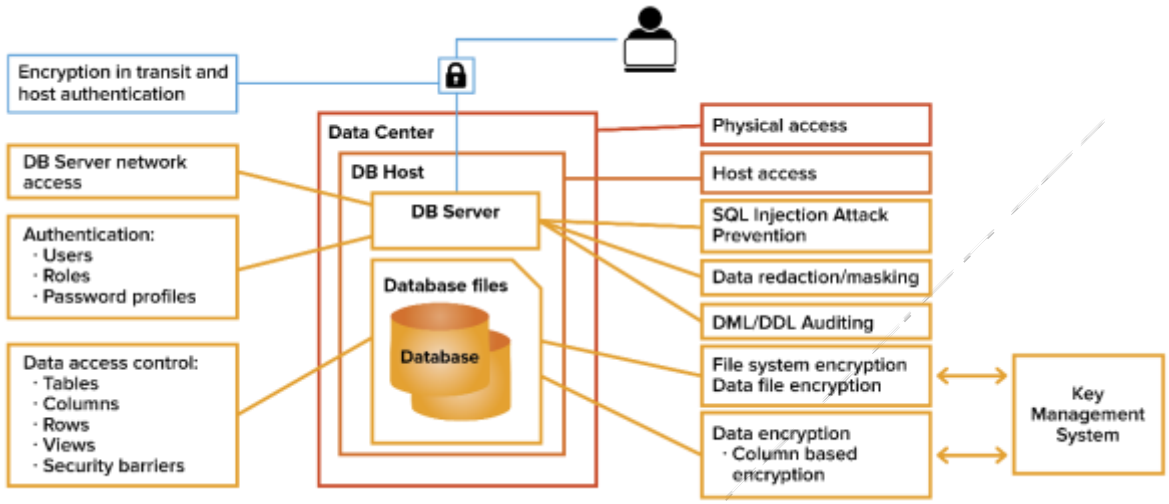

Fig 3.1. System Architecture

3.5 System Authentication Protocol

An authentication convention is a kind of PC correspondence convention or cryptographic convention which is utilized to move authentication data among customer and worker. This convention is fundamental for secure correspondence between the hubs in an organization. There are two fundamental kinds of authentication conventions, they are, Authentication conventions created for PPP and AAA engineering conventions (Authentication, Authorization, Accounting). This proposed framework utilizes AAA Architecture convention as Authentication convention. This is an unpredictable convention which is utilized in bigger organizations for approval, authentication and bookkeeping purposes.

Step 1. Authentication: Refers to who is allowed to gain access to the network (In this original clients of online banking). Clients are required to prove their identity.

Step 2. Authorization: Refers to what the client is allowed to do or what services the client access to.

Step 3. Accounting: Refers to keeping track of what the client did and what services were used. This is necessary for security auditing purposes of banks. Accounting uses start and stop of the messages to keep track of when a service was started and when it was terminated.

Terminal Access Control Access Control Server (TACACS+), Remote Authentication Dial-In User Service (RADIUS) and DIAMETER are the servers which utilizes the above Authentication protocol.

4.RESULTS

The idea of Steganography and the edge VCS is utilized. At that point, the Intermediary data set holds questions in regards to the real offer worth that is given as contribution by the User during Sign Up. For phishing assault recognizable proof and counteraction, the proposed framework utilizes another system. It forestalls the spillage of secret key and other classified data to the organization assault called Phishing by counterfeit look-a-like sites. Phishing website pages are produced site pages. It is made by pernicious individuals to mirror the Web pages of approved sites. This phony page has the most noteworthy visual likenesses to trick their casualties. These casualties of the 'Page – Phishing' may uncover their touchy data to the phishing page proprietors. Since this technique depends on the picture CAPTCHA approval conspire utilizing 'Steganography' and 'Visual Cryptography', its dependability is at an improved level.

Figure 4.1 Encryption page

Figure 4.2 Login Screen for bank

5.Comparative Analysis

Table 4.1 shows the diverse exhibition estimated by utilizing various boundaries. Condition is utilized to ascertain the precision, arrangement mistake and standard deviation of accessible dataset individually. Precision of strategic relapse is more noteworthy and arrangement

Sno	Algorithm	Length of keys	Accuracy
1	SHA	32 bits	79%
2	RSA	32 bits	75%
3	SHA1	64bits	83%
4	RSA2	64bits	76%
5	SHA+RSA(current)	128bits	90%

Table 4.1 Comparative analysis of various algorithms and their accuracy

As seen from the above table information, unmistakably the proposed calculation can deal with pictures of different classifications, record sizes, characteristics and goals. The size of the offers depends on the key size indicated in the encryption stage. Despite the fact that huge key record size isn't suggested, the calculation can deal with enormous key sizes also. This is because of the way that each and each key goes through a hashing instrument executed utilizing SHA-256. The hash size is consistently 256 paying little heed to the key size. Concerning the code text length, it has been noticed that length of the code created is around 1.5 occasions the size of the picture. This may represent an issue for higher quality pictures on account of the code text size. In such cases, the length of the code can be diminished utilizing hashing instruments or the information can be as encoded lumps where each piece is a piece of the picture, packed utilizing pressure calculations. Another conceivable answer for pack the picture before encryption, so that document size can be decreased relatively. Subsequently, the calculation is reasonable for sending compacted pictures in the organization and it ought to be altered in the event that one needs to send crude and great pictures. The cryptographic approach proposed in this paper has been tried on various sorts of information pictures with change in size of the picture and keys of AES

encryption calculation. The whole time secret picture is recovered with acceptable visual quality. Truth be told, there is no discernible change in the nature of picture, since the picture handling is for the most part done on the key pictures what's more, its offers. The secrecy of offers is likewise tried by changing the vital offers prior to coming to the objective. In every one of the cases it has been seen that if any gatecrasher will be fruitful in getting the encoded shares from organization, he or she can't recover the first mystery picture without accessibility of code. Additionally since the intricacy of the encryption is twofold layered the programmer couldn't in any way, shape or form get to realize the calculations utilized in the encryption. So it is still hard to break the visual cryptography regardless of whether the programmer gets his hands on the critical offers over the organization.

6.CONCLUSION

The blend of fingerprints biometric examine and the picture check can offer safer component for security. Interfacing the biometric filtering dongle to the worker, naturally check with the both Macintosh add of the dongle and username secret phrase of the record are coordinating. In addition, picture confirmation done by the client, to recognize the picture that given by the applicable bank. This is because of the reality to forestall obscure authentication loggings. Likewise, banking framework utilizing a PKI to get the sender and beneficiary record subtleties. All the logging subtleties will be shipped off authentication worker. Finally,‖ Improved E-banking System with Advanced Encryption Standards and security Models‖ progress between e-banking frameworks ought to be grown more and carried out to give security mindfulness, for example, cash moving dangers and dangers logging data to all current and potential web banking clients.

REFERENCES

[1]H. Ullah Khan, "E-Banking: Online Transaction and Security Measures", Research Journal of Applied Sciences, Engineering and Technology, vol. 07, no. 19, pp. 1-8, 2014[online]. Available at: http://maxwellsci.com/jp/abstract.php?jid=RJASET&no=428&abs=14 [Accessed 28 Jul. 2016].

[2]E. R.Nwogu, "Improving the security of the Internet Banking System Using Three-Level Security Implementation", International Journal of Computer Science and Information Technology and Security, vol. 04, no. 06, pp. 1-10, 2014[online]. Available at:http://ijcsits.org/papers/vol4no62014/7vol4no6.pdf [Accessed 28 Jul. 2016].

[3]K. Thamizhchelvy and G. Geetha, "E-Banking Security: Mitigating Online Threats Using Message Authentication Image (MAI) Algorithm", International Conference on Computing Sciences, pp. 1-5, 2012[online]. Available at: https://www.eecis.udel.edu/~wwang/cisc849/E-Banking%20Security%20Mitigating%20Online%20Threats%20Using%20Message%20Authentication.pdf [Accessed 28 Jul. 2016].

[4]Kovach S. and Vicente Ruggiero,"Online Banking Fraud Detection Based on Local and Global Behavior",The Fifth International Conference on Digital Society, pp. 1-6, 2011[online]. Available at: https://www.researchgate.net/publication/228616927_Online_Banking_Fraud_Detection_Based_on_Local_and_Global_Behavior [Accessed 16 Aug. 2016].

[5]Chen H. and Corriveau J"Security Testing and Compliance for Online Banking in Real-World",Proceedings of the International Multi Conference of Engineers and Computer Scientists, vol.

1, pp. 1-5, 2009 [online]. Available at:http://www.iaeng.org/publication/IMECS2009/IMECS2009_pp1039-1043.pdf [Accessed 14 Aug. 2016].

[6]D.S. Coming and O.G. Staadt, "Velocity-Aligned Discrete Oriented Polytopes for Dynamic Collision Detection," IEEE Trans. Visualization and Computer Graphics, vol.14, no.1, pp.1-12, Jan/Feb2008, doi:10.1109/TVCG.2007.70405. (IEEE Transactions)

[7]Khrais, Laith. "Highlighting The Vulnerabilities of Online Banking System". The Journal of InternetBanking and Commerce 2015 (2015): n. pag. Web. [online]. Available at: http://www.icommercecentral.com/open-access/highlighting-the-vulnerabilities-of-online-banking-system.php?aid=61518 [Accessed 08 Sep. 2016].

[8]Ula, Munirul, Zuraini Ismail, and Zailani Sidek. "A Framework for The Governance of Information Security in Banking System". JIACS (2011): 1-12[online]. Web. Available at: http://ibimapublishing.com/articles/JIACS/2016/726196/726196.pdf [Accessed 08 Sep. 2016].

[9]Das, Soumyajit and Dr. Pranam Dhar."Technological Security Aspects for Internet Banking". PARIPEX 3.6 (2012): 110-115. Web.

[10]A Haque, A zaki, "Issues of E-Banking Transaction: An Empirical Investigation On Malaysian Customers Perception". Connection.ebscohost.com. N.p., 2016. Web. Availableat: http://irep.iium.edu.my/8061/1/Issues_of_E-banking_transaction_An_empirical_investigation_on_Malaysian_customers_perception.pdf[Accessed :14 Sept. 2016.]

[11]Mohammadi, Shahriar and Sanaz Abedi. "ECC-Based Biometric Signature: A New Approach in Electronic Banking Security". 2008 International Symposium on Electronic Commerce and Security(2008): n. pag. Web. Available at: https://www.eecis.udel.edu/~wwang/cisc849/AshrafBah-Pres1-Paper2.pdf[Accessed:14 Sept. 2016.]

[12]Subsorn, P. and S. Limwiriyakul. "A Comparative Analysis of Internet Banking Security in Thailand: A Customer Perspective". Procedia Engineering32 (2012): 260-272. Web. Available at: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1024&context=icr[Accessed14 Sept. 2016.]

[13]S. Pakojwar and D. Uke, "Security in Online Banking Services –A Comparative Study", International Journal of Innovative Research in Science, Engineering and Technology, vol. 3, 2014[online].Availableat: http://www.ijirset.com/upload/2014/october/79_Security.pdf [Accessed 14 Sep. 2016].

[14]R. Kaur Jassal and R. Kumar Sehgal, "Online Banking Security Flaws", International Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, 2013[online].Availableat: http://www.ijarcsse.com/docs/papers/Volume_3/8_August2013/V3I2-0257.pdf [Accessed 14 Sep. 2016].

[15]J. Choubey and B. Choubey, "Secure User Authentication in Internet Banking: A Qualitative Survey", International Journal of Innovation, Management and Technology, vol. 4, 2013[online].Available at: http://www.ijimt.org/papers/391-D0493.pdf [Accessed 14 Sep. 2016].

[16] SozanAbdulla,"New Visual Cryptography Algorithm For Colored Image",JOURNAL OF COMPUTING, VOLUME 2, ISSUE 4, APRIL 2010, ISSN 2151-9617 HTTPS://SITES.GOOGLE.COM/SITE/JOURNALOFCOMPUTING/.

[17] InKoo Kang, Member, IEEE, Gonzalo R. Arce, Fellow, IEEE, and Heung-Kyu Lee, Member, IEEE"Color Extended Visual Cryptography Using Error Diffusion",IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 20, NO. 1, JANUARY 2011.

[18] DivyaJames,MintuPhilip,"A Novel Anti Phishing framework based on Visual Cryptography",2012 IEEE.

[19] Roberto De Prisco and Alfredo De Santis,"On the Relation of Random Grid and Deterministic Visual Cryptography",IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 9, NO. 4, APRIL 2014.

[20] XingxingJia, Daoshun Wang, Member, IEEE, DaxinNie, Chaoyang Zhang, Member, IEEE,"Collaborative Visual Cryptography Schemes",Transactions on Circuits and Systems for Video Technology, 2016.

[21] ShreyaZarkar, Sayalivaidya, ArifaTadvi, TanashreeChavan, Prof. AchalBharambe "Image Based Authentication Using Visual Cryptography and Encryption Algorithm ", International Journal of Computer Science and Information Technologies, Vol. 6 (2) , 2015, 1692-1696.

[22] Mrs. A . Angel Freeda ,M.Sindhuja , K.Sujitha"ImageCaptcha Based Authentication Using Visual Cryptography", International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 2 , April - May , 2013.

[23] DoshiRuchali 1 , Kale Prajakta 2 , PasalkarPranoti "Secured Transaction System Using Steganography and Visual Cryptography",2016 IJESC

[24] A. Shami r, "How To Share a Secret", Commun. ACM, vol. 22, pp. 612-613, 1979.

[25]G. R. Blakley, "Safe guarding cryptographic keys", in Proceedings of the 1979 AFIPS National Computer Conference, 1979, pp. 313- 317. [11]D.S. Wang, Z. W. Ye, and X.B. Li , "How to Collaborate bet ween Threshold Schemes", arXiv:1305.1146v1, pp. 1-14.

[26]M. Naor and A. Shamir, "Visual Cryptography", Adv. Cryptogr., pp. 1-12, 1995.

[27]C.N. Yang, "New visual secret sharing schemes using probabilistic method", Pattern Recognit. Lett., vol. 25, no. 4, pp. 481-494, 2004.

[28]S. Cimato, R. De Prisco, and A. De Santis, "Probabilistic visual cryptography schemes", Comput. J., vol. 49, no. 1, pp. 97-107, 2006.

[29] R.Biddle, S.Chiasson and P.C.Van Oorschot, “Graphical pass - words: Learning from the first twelve years,” ACM Comput. Surveys, vol. 44, no. 4, 2012.

[30] “Cognitive Authentication Schemes safe against Spyware” IEEE publication under security and privacy 2006 by Weinshall, D., Hebrew University of Jerusalem.