Research Paper E-ISSN NO : 2455-295X | VOLUME : 2 | ISSUE : 12 | DEC 2016

MULTIPLE SECRET SHARING WITH CIRCULAR SHARES OF VISUAL CRYPTOGRAPHY

Dr. G Lakshmeeswari [1] | P Chaitanya [2]
[1] GITAM University, Siddardha College Visakhapatnam, Vijayawada, AP

ABSTRACT

Visual Cryptography has its prominence in authentication applications. User authentication is the maiden requirement for a safe communication. The proposed technique hosts multiple secrets in two shares that are circular in shape and reveals the accurate information only on precise specification of stacking angle of the shares. This methodology is mainly aimed at producing meaningful information to the intruder and disguising him that his intrusion was successful. The right user is decided being on the disclosed content.

Keywords: Menarche, Height, Adolescents.

Introduction

Authenticating the receiver is important task for secure communication. Cryptography is widely used for secure data transmission via-Internet or through any type of networks. Organizations like Intelligence agencies around the world depend majorly on cryptographic methodologies for secure transmission of any type of message – offline or online. No online data is considered secure unless we encrypt it. Cryptography assures confidentiality, Integrity as well as Authentication. Visual Cryptography (VC) plays a vital role in authentication. It is used in innumerable applications for user authentication.

Visual Cryptography was initially proposed by Naor and Shamir[1]. Several studies have been proposed to improve the number of secrets that can be stored in the shares[5]. In order to minimize the distortions caused by different geographical shapes a secret sharing scheme using circular properties was proposed by L. Ge, S. Tang[4].

Authentication using VC Rotation Scheme

Authentication of the recipient is done in this system basing on the text revealed on rotating the share. Two circle shares namely Share A and Share B are considered. These shares are rotated at certain angle to generate the secret message. The angle at which rotation has to be made is a prior understanding between the sender and the receiver. Four secrets are shared in two shares and each secret is revealed on rotating the shares at an angle of 90 degrees.

- On stacking the Share A upon Share B with an initial angle, the first secret is revealed.
- The initial angle is given as input to the system and it need not necessarily be 0 degrees.
- Only 4 secrets are stored in the shares.
- Adding 90 degrees to the initial angle and rotating the Share B in clock wise direction reveals the second secret.
- Repeat the previous step two more times to reveal the other two secrets.

If the initial angle is considered as 0 degrees, the other angles at which the secret message would be present are 90, 180 and 270 degrees. If the initial angle is considered as 30 degrees then the other three angles would be 120, 210 and 300 degrees respectively. The initial angle is kept variant as a security measure. Figure 1 shows a sample image of the revealed secrets on rotating the share B at different angles.

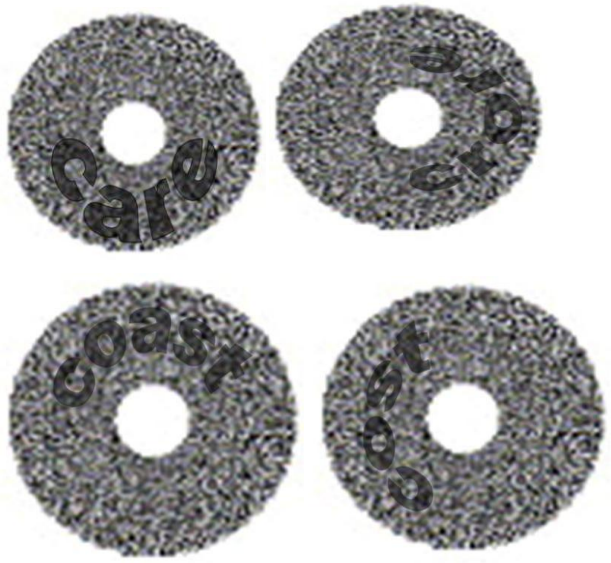

Figure 1: The revealed secrets present in the shares

The receiver has to give as input the angle at which the share has to be rotated. The information revealed on rotation is encrypted and transmitted to the sender. The sender on receiving the secret would compare it with the actual secret which has to be revealed and on satisfaction authenticates the recipient and the connection is established to transmit the Text. If the recipient fails to unveil the correct secret, the connection is denied and the session is terminated. The Recipient is given only a single chance to authenticate himself.

Higher levels of security is achieved if we authenticate the receiver first and then transmit the text. Authentication decides whether the receiver is the intended recipient or not, and on conformation from the authentication system only we establish a connection to transmit the data.

Conclusion

The proposed share rotation technique is designed for holding multiple secrets in two shares and confuse the users by giving meaningful secrets even though the initial stacking angle is inappropriate. This meaningful secrets make the intruder assume that his attempt was successful. The initial stacking angle is known only to the intended communicating parties. The probability of finding the appropriate stacking angle is 0.002. This methodology can also be used to transmit passwords.

REFERENCES

[1] M. Naor and A. Shamir "Visual cryptography", Lecture notes in Computer Science,(950):1–12, 1995.

[2] Tzuung-Her Chen, Chang-Sian Wu, Wei-Bin B. Lee, " A Novel Subliminal Channel Found in Visual Cryptography and its Application to Image Hiding" D.O.I: 10.1109/IIH-MSP.2007.51 Publication Year: 2007 , Page(s): 421 – 424.

[3] L. Ge, S. Tang, "Sharing Multi-secret Based on Circle Properties", 2008 International Conference on Computational Intelligence and Security".

[4] J. Weir, W-Q Yan, "Sharing Multiple Secrets Using Visual Cryptography", 978-1-244-3828-0/09/, 2009 IEEE.

[5] Z. Fu, B. Yu, "Research on Rotation Visual Cryptography Scheme", 2009, International Symposium on Information Engineering and Electronic Commerce.

[6] Hsien-Chu Wu, Chin-Chen Chang, Sharing visual multi-secrets using circle shares, Elsevier, Volume 28, Issue 1, July 2005, pp 123-135.

[7] Lakshmeeswari, G., Rajya Lakshmi, D., Lalitha Bhaskari, D.: Extended Encoding of Telugu Text for Hiding Compatibility. IJCA 30(5) , 2011

[8] Ateniese, G., Blundo, C., Santis, A.D., Stinson, D.R.: Extended capabilities for Visual Cryptography. Theoretical Computer Science 250(1-2), 143–161 (2001)

[9] Yu, B., Xu, X., Fang, L.: Multi-Secret sharing threshold Visual Cryptography Scheme. International Conference on Computational Intelligence and Security (2007)

[10] Lakshmeeswari, G., Rajya Lakshmi, D., Srinivas, Y.: A New Encoding Scheme of Telugu Text for Information Hiding. International Journal of Computational Intelligence Techniques 2(1), 26–28 (2011) ISSN: 0976–20466 & E-ISSN: 0976–0474.

[11] Lakshmeeswari, G., Rajya Lakshmi, D., Srinivas, G Hima Bindu: A Model for Encryption of Telugu Text using Visual Cryptography scheme, AISC 177, Springer Verlag Berlin Heidelberg, 2013.