Multi-level Steganography Based on Fuzzy Vault Systems and Secret Sharing Techniques

Katarzyna Koptyra and Marek R. Ogiela(✉)

Faculty of Electrical Engineering, Automatics,
Computer Science and Biomedical Engineering,
AGH University of Science and Technology,
30 Mickiewicza Ave., 30-059 Krakow, Poland
{kkoptyra,mogiela}@agh.edu.pl

Abstract. This paper presents a new technique of secret sharing in fuzzy vault system with use of multi-level steganography. Every hidden information on each level is linked with individual key used in embedding and revealing stages. Higher level secret is a share which is needed to reconstruct concealed data. It is possible that different shares contain various amount of information, what means that some of them may be more or less privileged. As a result, the secret can be decoded correctly in a number of ways. Therefore the main objective of this paper is to propose a system in which some users may hide additional shared secret in an inconspicuous manner.

Keywords: Secret sharing · Steganography · Fuzzy vault · Information hiding

1 Introduction

Nowadays some pieces of information are so important that they should be divided into parts and distributed to a few people as it is dangerous to accumulate so much secret data and responsibility in the hands of one person. This need resulted in continuous development of secret sharing algorithms. Some of these methods allow to graduate rights, what means that the secret can be correctly decoded in many ways, for example with use of lower number of more privileged shares or higher number of less privileged ones.

In practice there are cases where in multi-users system only a small group of people should have access to the secret message and remain users are not supposed to be aware of the existence of this information. The first solution which comes to mind is to create a brand new system available only for authorized users. Two main disadvantages of this idea are necessity of maintaining one more system and also problems with keeping its existence private. Thus one can try to create from scratch a new system, which first and overt functionality is to protect data owned by each individual user and second, covert feature is to keep hidden secret that is shared between authorized group of users.

This paper is the first attempt of initial proposal of such system. In its assumptions, the mechanism is built on three pillars: secret sharing algorithm, multi-secret fuzzy vault scheme, and multi-level steganography. These bases were described in Sect. 2,

J.J. Jung and P. Kim (Eds.): BDTA 2016, LNICST 194, pp. 115–121, 2017.
DOI: 10.1007/978-3-319-58967-1_13

while the system itself is presented in Sect. 3. Finally some conclusions and summary can be found in Sect. 4.

2 The Fundamentals of the System

To understand how proposed system works, the first important thing is to become familiar with its theoretical basis, which are: secret sharing, multi-secret fuzzy vault and multi-level steganography.

2.1 Secret Sharing

Secret sharing is an idea that allows to divide a secret into several parts (called shares or shadows) and distribute them to authorised participants [1]. To reconstruct the secret, a certain number of users have to cooperate and join their pieces. The number of shares below the threshold is unfeasible to make reconstruction [2]. Usually the shared secret is a number [2–4], sometimes may take different forms, like matrices [5, 6] or images [7–10]. It is possible to make hierarchical [4] or multistage systems [11]. In general, various algorithms may have additional features, for example larger number of shared secrets, ease of adding a new user, ease of changing the secret, verifiability or shadow reusability.

This type of information management has two main aims. Firstly, it removes single point of failure flaw, because the secret can be reconstructed even if some participants lose their shares. Secondly, it prevents from concentration of too much potential in the hands of one user, because no one can recover the secret alone.

2.2 Multi-secret Fuzzy Vault

Fuzzy vault is a type of cryptosystem based on polynomial reconstruction [12]. The whole system is made of a great number of points, from which some are genuine and remaining are noise. To unlock hidden information, right points have to be identified with use of a key that is in form of unordered set of numbers. On the basis of chosen points the user can reconstruct a polynomial with encoded secret (a number). Therefore the main idea of this system is to protect an information by placing it in a very noisy environment. In vault creation process some coefficients of polynomial are dependent on secret value, others are selected randomly. This polynomial is then used to obtain genuine points by evaluate the formula on all key values. Further lots of chaff points (not lying on polynomial) are generated randomly or with use of more sophisticated algorithms [13, 14].

The interesting feature of fuzzy vault scheme is its error tolerance. The user can decode the secret with use of similar, but not identical key. However, both keys have to overlap substantially, otherwise the obtained genuine points are not sufficient to reconstruct the polynomial. This property in combination with order-invariance opens the possibility of using keys derived from biometric traits [15].

Multi-secret fuzzy vault is an extension of described scheme which allows to hide more secrets [16]. Every number is encoded in its own polynomial and has individual key. The important assumption is that all keys are disjunctive (as they are still unordered sets). Another property that distinguishes multi-secret version from original one is false points generation method. In extended scheme chaff points cannot be positioned on any of polynomials. All remaining characteristics of fuzzy vault are preserved, including error tolerance and order invariance. It is worth to mention that above rules are suitable for single user with many secrets or for multi-users system, in which each participant has his own key.

2.3 Multi-level Steganography

Steganography is a technique of information hiding in which some secret data is embedded in an inconspicuous medium called container (carrier, cover) [17]. The main assumption is to prevent disclosure of the secret, because when its existence is revealed, the whole system failed [18]. Therefore every steganographic method is supposed to be highly undetectable against unauthorized recipients. Currently there is a wide selection of algorithms and various covers in this interesting field [19].

Multi-level steganography is a branch of such science which provides different levels of hiding. In other words, a container with embedded data become new message and is hidden in an another carrier. Usually each subsequent level requires more capacity. To extract the last information, one should first decode every secret from all previous levels. More about multi-level steganography may be found in [20, 21].

3 Multi-level Fuzzy Vault System for Secret Sharing and Steganography

This section describes main elements of the newly proposed system. At the beginning it is worth to remain main assumptions, which are as follows. The system is destined for multiple users and has two levels of information hiding. First level is available for every user who wants to protect one numeric secret. Keys are in form of disjunctive unordered sets. Second level is known only to an authorized group of users and stores one shared secret. To decode this information, a sufficient number of users has to cooperate and combine their parts. Two things are required for computing a share: 1^{st} level secret reconstruction and 2^{nd} level key (numeric).

Below are explained hiding and reconstruction phases with details of overt and covert levels.

3.1 Hiding Phase

Every normal user applies Algorithm 1 for locking his own secret. The covert level is known only to specific group and requires special method described in Algorithm 2. This technique conceals two secrets as they are related. In depicted algorithms the

assumption is that all polynomials are of degree n. All sets are indexed from 1, for instance 3-element set S can be denoted as (S_1, S_2, S_3).

Algorithm 1. Hiding secret (normal user)

Input: s – secret (numeric), k – key (set of numbers)
Output: v – set of points

1. Compute l as length of k
2. Randomly choose coefficients $a_n, a_{n-1}, \ldots, a_1$
3. Create a polynomial $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + s$
4. Evaluate p on elements of k, in other words compute $p(k_1), p(k_2), \ldots, p(k_l)$
5. Add all computed points $p(k_1), p(k_2), \ldots, p(k_l)$ to v
6. Return v

For authorized users, the polynomial p is generated in a different way. It is based on temporary polynomial q which conceals higher level secret. The difference between these two formulas become second level key. Again p and q have the same degree n which is equal the length of second level secret.

Algorithm 2. Hiding secret (initiated user)

Input: s – 1st level secret (numeric), k – 1st level key (set of numbers), S – share (set of numbers)
Output: v – set of points, K – 2nd level key

1. Randomly choose coefficient a
2. Create polynomial $q(x) = a(x - S_1)(x - S_2)\ldots(x - S_n)$
3. Compute canonical form of polynomial $q(x)=ax^n + ab_{n-1}x^{n-1} + \ldots + ab_1 x + ab_0$ where:
   $b_{n-1} = S_1 + S_2 + \ldots + S_n$
   $b_{n-2} = S_1S_2 + S_1S_3 + \ldots + S_1S_n + S_2S_3 + \ldots + S_{n-1}S_n$
   …
   $b_1 = S_1S_2\ldots S_{n-1} + S_1S_2\ldots S_{n-2}S_n + \ldots + S_2S_3\ldots S_n$
   $b_0 = S_1S_2\ldots S_n$
   Note: $b_{n-1}, b_{n-3}, \ldots$ are negative. So for odd n b_0 is negative and for even n b_1 is negative.
4. Compute $K = ab_0 - s$ (2nd level key)
5. Compute l as length of k
6. Create polynomial $p(x) = ax^n + ab_{n-1}x^{n-1} + \ldots + ab_1 x + s$
7. Evaluate p on elements of k, in other words compute $p(k_1), p(k_2), \ldots, p(k_l)$
8. Add all computed points $p(k_1), p(k_2), \ldots, p(k_l)$ to v
9. return K, v

After computing sets of points for all participants and keys for authorized users, chaff points are generated. There is one limitation in comparison to original fuzzy vault scheme. Here false points cannot lie on any of polynomials p. It does not matter if they

are located on a temporary polynomial q from algorithm 2. Finally all genuine and chaff points are gathered together to form a vault.

3.2 Reconstruction Phase

First level secret reconstruction is identical as in fuzzy vault scheme [12]. In short, the participant uses his key k to choose genuine points from entire vault. Then these points are used to reconstruct polynomial p. The secret s is read from free term of p. Obtaining data from second level is more complicated, therefore it is presented in algorithm 3.

Algorithm 3. Share reconstruction

Input: V – set of all points, k – key, K – 2nd level key
Output: S – share (set of numbers)

1. Use k to filter genuine points from V
2. Reconstruct polynomial p
3. Compute polynomial $q(x) = p(x) + K$
4. Write polynomial q in factored form $q(x) = a(x - S_1)(x – S2)…(x - S_n)$
5. Return S

As can be seen, each share is in form of set of numbers. This gives a chance of using them as a key in another fuzzy vault in which the secret is recovered as described in [12]. This selection is justified by an opportunity of reusing a part of the system as the method is identical as 1st level secret reconstruction (overt functionality of the system).

At the end of the section, it should be explained how it is possible to assign different privileges to users. The previous assumption was that all polynomials were of level n, which was also the length of each share. However, some parts may be weakened by placing redundant information inside. In other words, the reconstructed polynomial q has multiple roots and, as a result, some data in the share overlap. In a simple case with three users, key length = 3 and n = 2, we can assign following shares: User1 has (S1, S2), User2 has (S3, S3) and User3 has (S4, S4). In this scenario User1 has to cooperate with User2 or User3 (or with both of them), but User2 and User3 are not able to reconstruct the secret without User1, because their key has length 2.

4 Conclusions

This paper introduces a secret sharing system based on multi-secret fuzzy vault and multi-level steganography. Presented system offers two functionalities. First, overt, allows to protect one secret per user and is available for every participant. The second one is hidden and is known only to specific group of users who can share another concealed secret. Privileges can be graduated by creating shadows containing different amount of information. Additionally it is possible to set up various hierarchical structures and subgroups which have to cooperate, because some parts of the secret

may be present only in one of them. Moreover one system may contain independent authorized groups that share different secrets and are not informed about remaining ones.

Acknowledgments. This work was supported by the AGH University of Science and Technology research Grant No 15.11.120.868.

References

1. Martin, R.: Introduction to secret sharing schemes. Computer Science Department, Rochester Institute of Technology, Rochester (2012)
2. Shamir, A.: How to share a secret. Commun. ACM **22**, 612–613 (1979)
3. Blakley, G.F.: Safeguarding cryptographic keys. In: National Computer Conference, pp. 313–317 (1979)
4. Zhenjun, Y.: Construction and application of multi-degree secrecy system based on threshold secret sharing. In: International Conference on Power System Technology, PowerCon 2006, pp. 1–4 (2006)
5. Bai, L.: A strong ramp secret sharing scheme using matrix projection. In: International Symposium on World of Wireless, Mobile and Multimedia Networks, WoWMoM 2006, pp. 652–656 (2006)
6. Wang, K., Zou, X., Sui, Y.: A multiple secret sharing scheme based on matrix projection. In: 33rd Annual IEEE International Computer Software and Applications Conference, COMPSAC 2009, pp. 400–405 (2009)
7. Chien, M.C., Hwang, J.: Secret image sharing using (t,n) threshold scheme with lossless recovery. In: 2012 5th International Congress on Image and Signal Processing (CISP), pp. 1325–1329 (2012)
8. Chang, C.C., Kieu, T.D.: Secret sharing and information hiding by shadow images. In: Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIHMSP 2007, vol. 2, pp. 457–460 (2007)
9. Bai, L.: A reliable (k, n) image secret sharing scheme. In: 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing, pp. 31–36 (2006)
10. Nag, A., Singh, J., Sarkar, D., Sarkar, P., Biswas, S.: Distortion free secret image sharing based on x-or operation. In: 2012 International Conference on Communications, Devices and Intelligent Systems (CODIS), pp. 286–289 (2012)
11. He, J., Dawson, E.: Multistage secret sharing based on one-way function. Electron. Lett. **30** (19), 1591–1592 (1994)
12. Juels, A., Sudan, M.: A fuzzy vault scheme. Des. Codes Cryptography **38**(2), 237–257 (2006)
13. Hani, M.K., Marsono, M.N., Bakhteri, R.: Biometric encryption based on a fuzzy vault scheme with a fast chaff generation algorithm. Future Generation Comp. Syst. **29**, 800–810 (2013)
14. Nguyen, T.H., Wang, Y., Nguyen, T.N., Li, R.: A fingerprint fuzzy vault scheme using a fast chaff point generation algorithm. In: 2013 IEEE International Conference on Signal Processing, Communication and Computing (ICSPCC), pp. 1–6. IEEE (2013)
15. Nandakumar, A.K.J.K., Pankanti, S.: Fingerprint-based fuzzy vault: Implementation and performance. IEEE Trans. Inf. Forensics Secur. **2**, 744–757 (2007)

16. Koptyra, K., Ogiela, M.R.: Fuzzy vault schemes in multi-secret digital steganography. In: 10th International Conference on Broadband and Wireless Computing, Communication and Applications, BWCCA 2015, Krakow, Poland, 4–6 November 2015, pp. 183–186 (2015)
17. Bailey, K., Curran, K.: Steganography – The Art of Hiding Information. BookSurge Publishing, New York (2005)
18. Cox, I., Miller, M., Bloom, J., Fridrich, J., Kalker, T.: Digital Watermarking and Steganography. Morgan Kaufmann Publishers, San Francisco (2008)
19. Subhedar, M.S., Mankar, V.H.: Current status and key issues in image steganography: A survey. Comput. Sci. Rev. **13–14**, 95–113 (2014)
20. Ogiela, M.R., Koptyra, K.: False and multi-secret steganography in digital images. Soft. Comput. **19**(11), 3331–3339 (2015)
21. Tang, M., Hu, J., Song, W.: A high capacity image steganography using multi-layer embedding. Optik – Int. J. Light Electron Opt. **125**(15), 3972–3976 (2014)