Securing Barcodes Using Compressed Secret Sharing Scheme

Kiran R. Chaudhari
ME Scholar
Pimpri Chinchwad College of Engineering
Pune-411044

Sonali Patil
Assistant Professor
Pimpri Chinchwad College of Engineering
Pune-411044

ABSTRACT
Bar code provides convenient way for people labeling a tag on a product so that people can easily and quickly identify the content of product itself. Large information of any product can be store in the form of bar codes which reduces the size of data. When this bar code contains important data or privacy information, the risk of security becomes an important problem. This paper proposes a secret sharing mechanism to enhance the security and data privacy for bar codes. The proposed technique uses Thein and Lin's image secret sharing to improves barcode image security during transmission. It also provides compressed shares of the barcode which reduces overhead of bandwidth in the network.

Keywords
Barcodes, Secret Sharing, Information Security, Network Security.

1. INTRODUCTION
Now a day's bar codes play a vital role in all the fields like grocery shops, airline inspection, book stores and etc. where the large data is converted into barcodes so that space complexity is reduced in database. And after scanning this bar codes people can easily and quickly identify the content of that product. The one dimensional (1D) barcodes is nothing but combination of different width of lines and spaces to represent data. The examples of these types of barcodes are code 39, code 128, EAN-13, ISBN etc.

1D barcodes is product identification and it is said that security of these barcodes are very low since they are easy to read by scanning the lines and the spaces, so to increase the security of these barcodes secret sharing scheme is used here.

The security of barcodes can be enhanced using secret sharing technique. The important data which is converted into barcode is converted into shares using the secret sharing techniques. The created shares are distributed among number of participants. The secret is recovered only when required number of participants comes together. The reduced size share reduces the space complexity.

The remaining part of the paper is organized in different sections as follows. The literature survey is given in Section 1. In Section 2 the proposed technique with system architecture is explained. Section 4 the comparative results. Conclusion is given in Section 5.

2. LITERATURE SURVEY
In this section various secret sharing schemes discussed. It includes Shamir's secret sharing scheme, Thien and Lin's image secret sharing scheme.

2.1 Shamir's Secret Sharing Scheme
Secret Sharing is a required nowadays in various fields for data security and this is protected against data leakage and loss.

Concept of secret sharing firstly invented by Adi Shamir [1] and George Blakley [2] in 1979 independently. Scheme proposed by both is based on different concepts. Shamir's scheme is based on polynomial technique while Blakley's scheme based on hyper plane concept. Secret sharing includes two main phases namely share construction and secret reconstruction phase. Shamir's scheme works as follows.

Share Construction
For share construction, threshold (k, n) and secret value S is required. Then polynomial function of an order (k-1) is constructed as shown in equation (1).

$$f(x) = d_0 + d_1 + d_2x^2 + \cdots + d_{k-1}x^{k-1}(mod\ p) \text{.....(1)}$$

In above equation, constant term *d0* is replaced with secret value S. The other coefficients such as, $d_1, d_2, \ldots, d_{k-1}$ are any random values.

Secret shares are the pairs of values.

(xi , yi), where *yi=f(xi)* for $1 \leq i \leq n$ and $0 < x1 < x2 \ldots < xn < n-1$.

After share construction polynomial function f(x) is destroyed and shares are distributed among n number of participants.

Secret Reconstruction
During secret reconstruction any k shares are collected. Then, secret value is computed using Lagrange's interpolation formula.

Equation (2) shows the Lagrange's interpolation formula which gives polynomial function f(x).

$$f(x) = \sum_{j=1}^{k} \left(y_{i_j} \prod 1 < -t < -k, t \neq j \ \frac{x - x_{i_t}}{x_{i_t} - x_{i_j}}\right) \bmod p \ldots\ldots (2)$$

The constant term in equation f(x) is our original secret value. Equation (2) can be further simplified as whole equation is not needed. Simplified equation is shown in equation (3) which directly gives constant term i.e. secret value S

$$d_0 = \sum_{j=1}^{k} \left(y_{i_j} \prod 1 < -t < -k, t \neq j \ \frac{x - x_{i_t}}{x_{i_t} - x_{i_j}}\right) \bmod p \ldots\ldots (3)$$

However, Shamir's scheme has two problems: large storage is required to retain all the shares, and heavy computational cost is needed to make shares and recover the secret due to processing a (k − 1)-degree polynomial.

2.2 Thien and Lin's Secret Sharing Scheme

Thien and Lin proposed image secret sharing scheme. It is mainly based on concept of Shamir's secret sharing scheme. In Shamir's scheme, (k-1) random numbers and the secret value together form the polynomial equation f(x). Thien and Lin suggested that instead of taking (k-1) random numbers pick k image pixels. It works as follows.

Share Construction

i. Read secret image S.

ii. Supress all pixels values to 250, which are greater than 250.

iii. Permute the secret image S.

iv. Sequentially take distinct k pixels of image S which are not already taken and form polynomial equation of order (k-1).

v. Then generate n pixels for n shadow images.

vi. Repeat steps (iv) and (v) until all pixels of image not get covered.

vii. Distribute n shadows among participants.

Secret Reconstruction

i. Collect any distinct k shadow images.

ii. Pick first but not yet used pixel from each shadow image.

iii. Using Lagrange's interpolation formula as shown in equation (2) get the coefficients of polynomial function f(x).

iv. Place these coefficients sequentially to form permuted image.

v. Pixels of permuted image inversely permuted to get the original one.

This scheme may give some distorted secret because of pixel suppression. Thien and Lin also proposed lossless image secret sharing scheme. In lossless scheme we have to keep track of pixels whose values are greater than 250.

2.3 A Novel Secret sharing technique using QR code

The authors Chou, Hu and Ko [3] proposed a novel secret sharing scheme using QR code using Shamir's secret sharing algorithm. The technique shares a confidential data into shadows (also called as shares) and one shadow is embedded into one tag or participants. No individual can recover the secret using its own share. The secret can be recovered only when the number of shadows is larger than or equal to a threshold.

But here the size of shares is same as that of barcode size.

3. PROPOSED TECHNIQUE

In this section, the brief discussion about the proposed theory, followed by proposed system architecture, where firstly the large data of any product is converted into bar codes.

Share Construction

i. Large data of any product is converted into required bar codes using the tool TRbarcode office in Microsoft office.

ii. Read this bar code as an image and this image will be considered as secret image.

iii. Using the Thein and Lin's secret sharing scheme make the shares of this image.

iv. Distribute these shares among the participants.

Share Reconstruction

i. Collect any distinct shares.

ii. Combination of these shares will give the desired barcode.

iii. This barcode later on after scanning will give the data of product.

The share size is compressed than the original secret. So there is less possibility of guessing the secret, here *t (k, n)* these shares are given to number of *n* participants where if the participants individually try to encrypt or generate the secret barcode they will fail to do it. As to recover or reconstruct the secret image, more than two participants should come together. Later on the secret barcode is reconstructed and from that barcode the data is read.

The space complexity is reduced here in two ways, firstly the large data of any product is converted and stores in the form of barcodes. Secondly, the shares generated here are compressed to that of secret image.

4. SYSTEM ARCHITECTURE

As discussed above, the procedure of the proposed system the system architecture is given below.

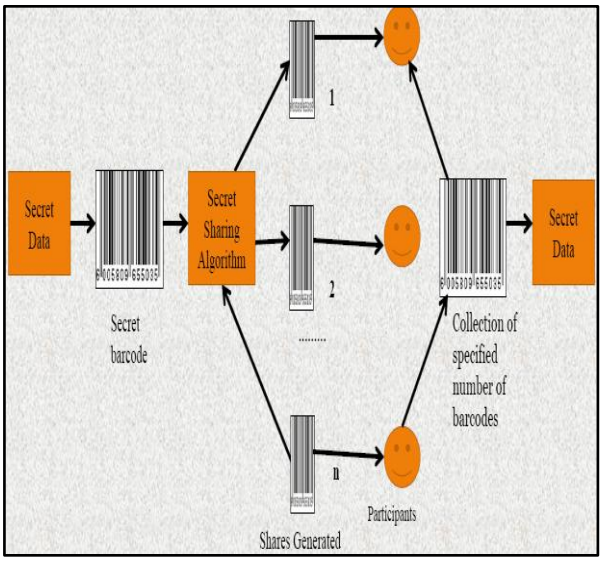

Fig 1: System Architecture

5. RESULTS

Results are calculated in following ways

Original Size data	**Barcode Size**	**Share Size [1]**	**Share Size by proposed Scheme t[2,4]**
14 kb (874 Characters)	9 kb	9 k	755 bytes
15kb (1000 Characters)	12 kb	12 kb	840 bytes
16 kb (1500 Characters)	14 kb	14 kb	872 bytes
18 kb (2035 Characters)	16 kb	16 kb	900 tes

6. CONCLUSION

In this paper, a secret sharing technique is implemented to enhance the security, data privacy and transmission for bar codes is proposed. This mechanism reduces the space complexity of the shares. This technique can be applied to various applications like airline luggage inspection, speed post, electronic tickets and other many fields.

7. ACKNOWLEDGMENT

The authors gratefully acknowledge the support provided to this study by National Chemical Laboratory, Pune.

8. REFERENCES

[1] Adi Shamir, “How to share a secret", Communication of the ACM, Volume 22, No. 11, PP. 612- 613, Nov 1979.

[2] G. R. Blakey, “Safeguarding Cryptographic Keys”, Proceedings of National Computer Conference, American Federation of Information, 1979.

[3] Jun-Chou Chuang, Yu-Chen Hu & Hsien-Ju Ko, “A Novel Secret Sharing Technique Using QR Code,” International Journal of Image Processing (IJIP), Volume (4): Issue (5), pp.468-475.

[4] M. Karthikeyan and Andreas Bender, “Encoding and Decoding Graphical Chemical Structures as Two-Dimensional (PDF417)Barcodes,” J. Chem. Inf. Model. 2005, 45,pp- 572-580

[5] T. Chen, “The application of bar code forgery - proof technology in the product sales management”. In Proceedings of the Intelligent Information Technology Application Workshops, Washington, DC, USA, 2008.

[6] Y. L. Yeh, J. C. You, and G. J. Jong, “The 2D bar-code technology applications in medical information management”. In Proceedings of the Intelligent Systems Design and Applications, Kaohsiung, Taiwan, 2008.

[7] A Jun Kurihara, Shinsaku Kiyomoto, Kazuhide Fukushima, and Toshiaki Tanaka “New (k, n)-Threshold Secret Sharing Scheme and Its Extension”