Verifiable Multi Secret Sharing Scheme for 3D Models

Jani Anbarasi[1] and Anandha Mala[2]
[1]Department of CSE, Anna University, India
[2]Department of Computer Science and Engineering, Easwari Engineering College, India

Abstract: *An efficient, computationally secure, verifiable (t, n) multi secret sharing scheme, based on YCH is proposed for multiple 3D models. The (t, n) scheme shares the 3D secrets among n participants, such that shares less than t cannot reveal the secret. The experimental results provide sufficient protection to 3D models. The feasibility and the security of the proposed system are demonstrated on various 3D models. The simulation results show that the secrets are retrieved from the shares without any loss*

Keywords: *Visual secret sharing, 3D graphics, cryptography.*

Received March 2, 2013; accepted June 9, 2014; published online August 25, 2015

1. Introduction

Visual secret sharing is an encryption technique, where a secret image is cryptographically encoded into *n* cipher images called shares. In (*t*, *n*) secret sharing scheme, the secret can be retrieved only with the help of *t* or more shares. By inspecting less than *t* shares, no information about the secret image is obtained. One of the great challenges in data security is to design efficient algorithms that are necessary to keep the system secure, particularly when transferring data through untrusted networks like internet. In ordinary encryption schemes, the encrypted data is placed in a single location. But if hacker finds the loop holes, it is easy to hack the information from the centralized storage and harm the secret, thereby affecting the integrity and confidentiality of the data.

Rapid development in computer and information technology has increased the use of 3D models in various areas, like manufacturing, medical imaging, virtual reality, computer games animation, etc., Studies say that people are more willing to license a product, if they can see how it works digitally, when not physically available for inspection. So, the protection of these 3D models is highly essential. Plenty of research work has been carried out to design robust and secure 2D image protection schemes, but 3D models have received less attention. The proposed secret sharing scheme offers efficient protection for the 3D models. So far many 2D image protection schemes like Steganography and other encryption schemes have been proposed. Shamir [10] first proposed the secret sharing scheme, which uses Lagrange's Interpolation polynomial. Blakley [1] proposed a secret sharing scheme based on the intersection of affine hyper planes. Several mathematical models have been proposed for text and numeric data encryption. These techniques are not suitable for multimedia related data because of their unique nature of pixel correlation and huge data.

In the last decade, various algorithms based on Shamir [10] have been proposed such as [8, 9, 13, 15]. Most of the generated shares have the same size as that of the secret. Very few algorithms generated smaller sized shares. Thien and Lin [13] generated shares of size 1/*t* of that of secret images. Using the Huffman encoding, Wang and Su [15] generated shares which are 40% smaller than the [13] approach. Meaningless shares are generated by these algorithms. Since, meaningless shares are being attracted by eavesdroppers they are embedded into a host image, and stego images using the steganography technique as in [2, 7, 15]. The meaningful shares avoid the suspicion of intruders.

In verifiable multi secret sharing scheme, any cheating by a dealer or by a participant can be detected as in [4, 5, 6, 12, 14, 16]. Shao and Gao [11] proposed a verifiable multi secret sharing based on YCH, where the shares should be distributed over a secure channel. Zhoa *et al.* [18] proposed a practical verifiable multi secret sharing scheme; which uses the RSA and Diffie Hellman concepts, where the shares are verifiable by both the participants and the dealer. In this paper, we present a verifiable multi secret sharing scheme for multiple 3D objects, based on the YCH scheme which uses [17] the RSA and Diffie Hellman key agreement concepts. This provides the verifiable property for both the dealer and the participants and property for both the dealer and the participants, and also avoids the necessity of the covert channel. 3D models are used in various areas, like manufacturing, military, virtual reality computer games, entertainment etc., less attention is given to 3D models, because the encryption schemes proposed for 2D images do not suit for 3D models.

The rest of the paper is organized as follows. In section 2, the traditional image secret sharing schemes are discussed. The proposed algorithmic methods of secret sharing approach for multiple 3D models are discussed in section 3. In section 4, the simulation results on various 3D models are provided. The analysis and conclusion are given in section 5.

2. Related Works

2.1. Multiple Secret Sharing Schemes

Shamir's secret sharing approach uses a secret *S* and a prime number m to generate a $(t\text{-}1)^{th}$ degree polynomial, which is given below:

$$h(x) = S + c_1 x^1 + \cdots c_{t-1} x^{t-1} mod\ m \tag{1}$$

The Coefficients are random integers within the range [0, *m*-1]. Yang *et al.* [17] proposed a multi secret sharing scheme along with a one way function *f(r, k)*. The function *f(r, k)* denotes any two variable one-way function that map a secret key *k* and a random value *r* onto a bit string *f(r, k)* of a fixed length. If *r* and *k* are given it is easy to compute *f(r, k)*. However, it is hard to compute:

- *r*: Given k and *f*(*r*, *k*).
- *f*(*r*, *k*): For any *r*, without any knowledge of *s*.
- *k*: Given *r* and *f*(*r*, *k*).
- *f*(*r'*, *k*): For $r' \neq r_i$, given pairs of r_i and $f(r, k_i)$.
- r_1 and r_2: Such that $f(r_1, k) \neq f(r_2, k)$, given *k*.

Here, $S_1, S_2, ..., S_p$ denotes *P* secrets to be shared among n participants. Initially, the dealer chooses n secret keys $k_1, k_2, \ldots, k_n$ in a random manner, and issues them to *n* authenticated participants by a covert channel. Then, the dealer performs the following steps:

- If ($p \leq t$):
  1. Choose a prime m and construct $(t\text{-}1)^{th}$ degree polynomial *h*(*x*) *mod m*, where $0< S_1, S_2, ..., S_p, c_1, c_2, ..., c_{t\text{-}p} <m$ as follows:

     $$h(x) = S_1 + S_2 x^1 + \cdots + S_p x^{p-1} + c_1 x^p + \cdots + c_{t-p} x^{t-1} mod\ m \tag{2}$$

  2. Compute $Y_i = h(f(r, k_i))$ *mod m* for *i*=1, 2, ..., *n*.
  3. Distribute (r, Y_i) to the participants.
- If ($p>t$):
  1. Choose a prime m satisfying $S_1, S_2, ..., S_p <m$, then construct the following $(p-1)^{th}$ degree polynomial:

     $$h(x) = S_1 + S_2 x^1 + \cdots + S_p x^{p-1} mod\ m \tag{3}$$

  2. Compute $Y_i = h(f(r, k_i))$ *mod m* for *i*=1, 2, ..., *n*.
  3. Compute *h*(*i*) *mod m* for *i*= 1, 2, ..., *p*−*t*.
  4. Distribute (r, Y_i, *h*(*i*)) to the participants.

For a (*t*, *n*) threshold scheme, we need at least t or more participants' secret shares to recover the *p* secrets $S_1, S_2, ..., S_p$. These participants pool their shares Y_i based on which the polynomial *h*(*x*) mod m can be determined uniquely as follows:

- **Case** ($P \leq t$):

$$h(x) = \sum_{i=1}^{t} Y_i \prod_{j=1, j\neq 1}^{t} \frac{x - f(r,k_i)}{f(r,k_i) - f(r,k_i)} mod\ m \tag{4}$$

- **Case** ($P>t$):

$$h(x) = Z_1 + Z_2 mod\ m$$

$$Z_1 = \sum_{i=1}^{t} Y_i \prod_{j=1, j\neq 1}^{t} \frac{x - f(r,k_i)}{f(r,k_i) - f(r,k_i)} \tag{5}$$

$$Z_2 = \sum_{i=1}^{p-t} h(i) \prod_{j=1, j\neq i}^{p-t} \frac{x - j}{i - j}$$

2.2. 3D Modelling

3D modelling is based on geometry, which is concerned with spatial relationships, particularly analytical geometry, which expresses these relationships in terms of algebraic formulae. Every point in a 3D model has three coordinates, which are called as axes labelled as (*x*, *y*, *z*), where *x*, *y*, *z* represent the height, length and breadth respectively.

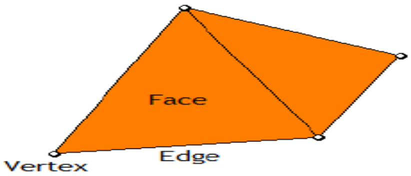


Figure 1. Graphical model.

The values of *x*, *y* and *z* will be in the range or correspond to 0<=*x*<=*H*, 0<=*y*<=*L*, 0<=*z*<=*B* where *H*, *L*, and *B* are the maximum height, length and breadth respectively. Generally, 3D models are represented as a mesh or polygons. A mesh is a collection of vertices, edges, and faces that describe the shape of a 3D object. A vertex is a point in the 3D model. An edge is a straight line connecting any two vertices. A face is a flat surface enclosed by edges. A face is any of the polygons of the 3D model that makes up its boundaries. Meshes can be represented in different ways based on how the vertices, edge and face information are stored.

3. Proposed 3D Secret Sharing Scheme

This paper propose *a*(*t*, *n*) threshold multiple 3D model secret sharing scheme with a verifiability property, in which multiple 3D models are shared among n participants as n distinct shares, where *t* participants can pool their secret shares to reconstruct the multiple 3D models, but less than *t* participants cannot recover the 3D models. All the 3D models should have the same number of vertices and faces. Secret keys are computed by both the participants and the dealer. The participants choose their own private key, and compute a secret value and provide it to the dealer. The dealer computes the secret key using a public key cryptosystem, and using this secret key in an invertible polynomial, the shares are generated and distributed to the participants. These generated shares have the same number of vertices and faces as those of the secret models. During recovery, the secret models are reconstructed by pooling the *t* shares using Lagrange's interpolation technique. Any cheating by the dealer and the participant can be prevented by the verification of the secret keys.

Generally, 3D models are represented as a mesh, where mesh *M* is defined as (*V*, *F*), where *V* represents the set of vertices and F represents the set of faces.

$$V = \begin{pmatrix} V_1 \\ V_2 \\ . \\ V_w \end{pmatrix} = \begin{pmatrix} v_{1x} & v_{1y} & v_{1z} \\ v_{2x} & v_{2y} & v_{2z} \\ . & . & . \\ v_{wx} & v_{wy} & v_{wz} \end{pmatrix}$$

$$F = \begin{pmatrix} F_1 \\ F_2 \\ . \\ F_m \end{pmatrix} = \begin{pmatrix} f_{1x} & f_{1y} & f_{1z} \\ f_{2x} & f_{2y} & f_{2z} \\ . & . & . \\ f_{mx} & f_{my} & f_{mz} \end{pmatrix}$$

Let $V=(v_1, v_{2;} ..., v_w)$ be the set of vertices and $F=(f_1, f_2, ..., f_m)$ be the set of faces.

3.1. Multiple 3D Secret Sharing using Shamir's Scheme

The proposed multiple 3D model secret sharing schemes has 3 phases; the initialization phase, the share construction phase and the verification and reconstruction phase. The initialization phase is divided into two processes: Secret key generation by the participants and secret key generation by the dealer. The usage of the key makes the encryption scheme more secure in the share construction phase; the secret shares are constructed using the YCH method, and in the reconstruction phase the verification of the shares is done by both the participants and the dealer in order to avoid cheating. Then, the original 3D models are are recovered by pooling the secret shares of *t* participants, using Equations 4 and 5. In place of *f(r, k_i) the* secret key I_i computed by the dealer is used in this scheme. The computations are done in a prime field F_p, which is the number of vertices of the 3D model. In this scheme, since the vertex coordinates have negative numbers, decimals and integers, it is very difficult to attack or predict the values. All the 3D models used for encryption should have the same number of vertices and faces. In order to avoid statistical attack; a duplication of the last vertex and the faces is done. A brief review of each phase is given below.

3.1.1. Initialization Phase

During the Initialization phase, the dealer and the participants need some intercommunication to share the secret keys for share construction [18]. The dealer chooses two large prime numbers *B* and *Q*, and computes *N*=*BQ*. The prime *B* and *Q* are chosen, such that *N* cannot be factorized effectively. An integer *g* is randomly chosen from the period $[N^{½}, N]$ by the dealer, such that *g* is relatively prime to *B* and *Q*. Then, the dealer distributes {*g*, *N*} to each participant.

Each participant U_i randomly chooses an integer K_i from the period [2, *N*] as his own secret keys and computes:

$$L_i = g^{k_i} \bmod N \tag{6}$$

Then, the participants provide a secret key L_i and their identity Id_i to the dealer. The dealer must ensure that secret keys $L_i \neq L_j$ for all participants $U_i \neq U_j$. If secret key $L_i = L_j$, the dealer should insist on the participants to choose distinct secret keys. The dealer chooses an integer S_0 from the period [2, *N*] arbitrarily, such that S_0 is relatively prime to (*B*-1) and (*Q*-1). The dealer then computes *f* as follows:

$$S_0 \times f = 1 \bmod \phi(N) \tag{7}$$

Where $\phi(N)$ is the Euler's phi-function. Then, the dealer computes:

$$R_0 = g^{S_0} \bmod N \tag{8}$$

$$I_i = L_i^{S_0} \bmod N \quad \text{for } i=1, 2, ..., n \tag{9}$$

And distributes the $\{R_0, f\}$ to each participant U_i ($1\leq i\leq n$).

3.1.2. Construction Phase

Secret shares are constructed from the multiple models for two cases, using the invertible polynomial.

- The number of secret 3D models is less than or equal to the threshold ($p\leq t$).
- The number of secret 3D models is greater than the threshold ($p>t$).

The steps to be followed to generate the shares for the two cases are given below:

- **Case** (***p*≤ *t***): Where the number of secrets is less than or equal to the threshold.

  1. The number of vertices F_p is used as the prime field and construct the $(t\text{-}1)^{th}$ degree polynomial $h(x) \bmod F_p$, where $0<S_1, S_2, \ldots, S_p, c_1, c_2, \ldots, c_{t-p} <F_p$ as follows:

$$h(x)=S_1+S_2x^1+...+S_px^{p-1}+c_1x^p+...+ c_2x^{p+1} +...+c_{t-p}x^{t-1} \bmod F_p \tag{10}$$

  2. Compute $Y_i(I_i) \bmod F_p$ for *i*=1, 2…, *n*.
  3. Distribute the (R_0, *f*, Y_i) to the participants.

- **Case** (*p*>*t*): Where the number of secrets is greater than the threshold.

  1. Choose the prime F_p and construct the $(k\text{-}1)^{th}$ degree polynomial $h(x) \bmod F_p$, where $0< S_1,S_2, \ldots, S_p<F_p$ as follows:

$$h(x) = S_1+S_2x^1+...+ S_px^{p-1} \bmod F_p \tag{11}$$

  2. Compute $Y_i(I_i) \bmod F_p$ for i=1, 2, …, *n*.
  3. Compute $h(i) \bmod F_p$ for i=1, 2, …, *p-t*.
  4. Distribute the (R_0, *f*, Y_i, *h*(*i*)) to the participants.

The mathematical model of the share creation is given in Figure 2.

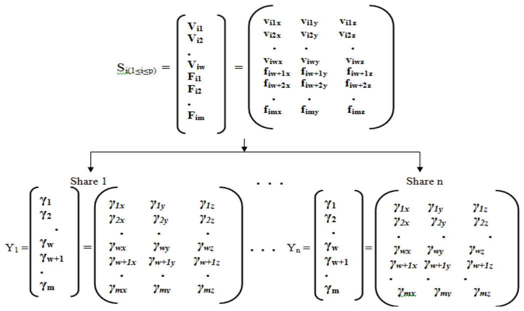


Figure 2. Representation of secret share having w vertices and m faces.

3.1.3. Recovery Phase

Participants pool their shares to recover the secret models S_1, S_2, ..., S_p. The secret models are reconstructed when t or more shares are processed using Equations 4 and 5 for both the cases and less than t shares cannot retrieve any secrets. In place of $f(r, k_i)$ the secret key I_i computed by the dealer is used in this scheme. Before pooling the shares each participant and the dealer can verify the shares of the others.

- Verification Process: Each participant U_i computes the secret key I_i'.

$$I_i{}' = R_0^{K_i} \mod N \qquad (12)$$

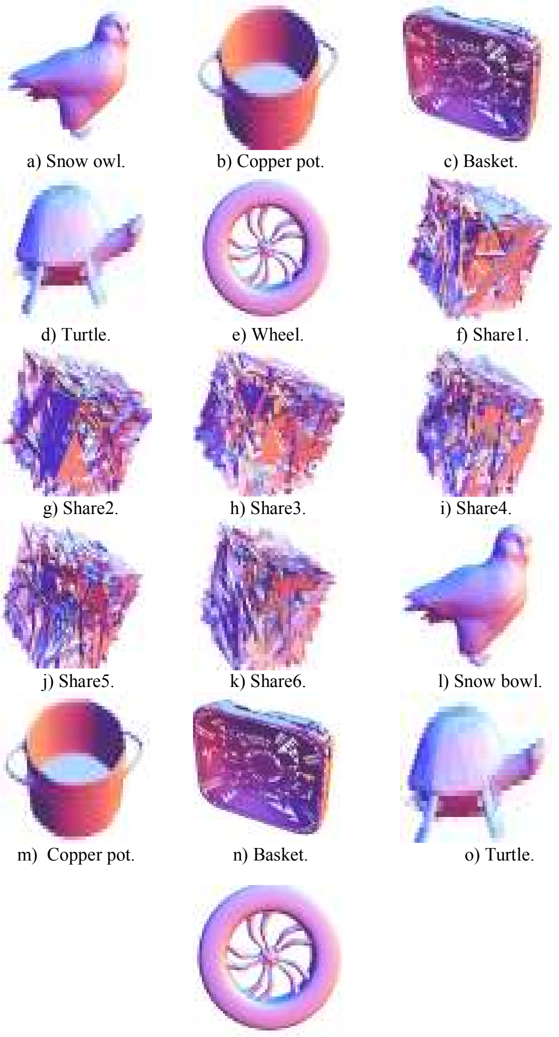
Where K_i is the private key of participant U_i.

Participants U_j ($U_i \neq U_j$) can verify the secret key I_i' provided by the participant U_i ; if $I_i'^{f} = L_i$ mod N, then secret key I_i' is true, otherwise I_i' is false and the participant U_i may be a cheat. The dealer can verify the secret key I_i' provided by the participant U_i; if $I'^{f}_i = I_i$, I_i' is true, otherwise secret key I_i' is false and the participant U_i may be a cheat, where the I_i secret value is computed by the dealer. The verification property prevents a participant from cheating the other participants and the dealer; that is, the dealer compares the secret keys whether $I'_{i=}\ I_{i;}$ if both are not equal, the dealer concludes that the participant is a cheat and each participant can verify the keys using $I'^{f}_i = L_i \ mod\ N$. Since, the participants choose their own secret keys K_i, the dealer cannot cheat the participants.

4. Experimental Results

The implementation is performed in Matlab 7.9 and Mathematica tool was used to viewing the 3D models. *A* (3, 6) threshold secret sharing scheme for multiple 3D models is implemented for both the cases $P \leq t$ and $P > t$, where P is the number of secret 3D models and t is the threshold. All the secrets are chosen to have the same number of vertices and faces; a few models are duplicated with the last vertex and face values, in order to have the same number of vertices and faces. If the number of vertices is not a prime number, then the last vertex is duplicated, until a prime number of vertices is reached.

Various models of varying sizes are tested for good results. For the first case ($p > t$), we have chosen various multiple secrets grouped under same number of vertices and faces. 6 secret models such as, snow owl, turtle, copper pot, wheel models and Basket, each with 4049 vertices and 12941 faces are chosen. The chosen prime value F_p for the generation of shares is 4049, which is the maximum vertex available in these models. Each of the vertices and faces is processed using the generated keys in the polynomial, and six shares are created and distributed to the participants as a text file.



a) Snow owl. b) Copper pot. c) Basket.

d) Turtle. e) Wheel. f) Share1.

g) Share2. h) Share3. i) Share4.

j) Share5. k) Share6. l) Snow bowl.

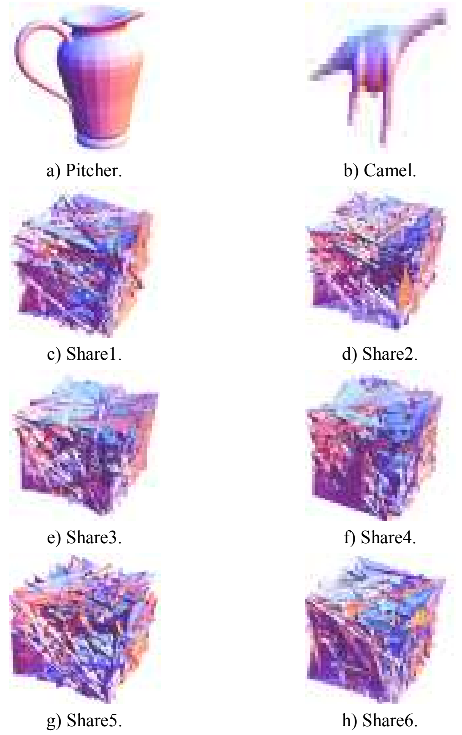
m) Copper pot. n) Basket. o) Turtle.

p) Wheel.

Figure 3. Secret 3D models and its generated shares for the case P>t.

Table 1. Comparison between sizes of various secret 3D models and the generated shares for the case secret less than the threshold (p≤t).

S. No	3D Model	3D Size(in Kb)	Prime	Share Size(in Kb)
1	Ghoul obj	139	2417	166
	TVs Spaceship	166		
2	Pleasure Craft	288	5231	290
	Camel	333		
3	Bronto	535	12763	745
	Pitcher	726		
4	T30	2225	35797	2045
	Trinity	2046		
5	Alexandria21	4101	98689	5145
	Tree1obj	4925		



a) Pitcher. b) Camel.

c) Share1. d) Share2.

e) Share3. f) Share4.

g) Share5. h) Share6.

Figure 4. (a)-(b) Secret 3D models and its Generated Shares for the case P≤t.

Table 2. Comparison between sizes for the case secret greater than the threshold (p>t).

S. No	3D Model	3D Size(in Kb)	Prime F_p	Share Size(in Kb)
1	Greyhound	60	1907	86
	Locust	87		
	Rabbit	83		
	Tiger	94		
	Zebra	78		
2	Basket	357	4049	293
	Copper Pot	209		
	Snow Bowl	283		
	Turtle	300		
	Wheel2	226		
3	Cappellinifelt Chair	440	8963	470
	Plastic Chair	479		
	Telephone Table	429		
	Zanotta Leonarda	445		
	High Ball Glass	390		
4	Deesawat Leaf Bench	440	9431	564
	Horse	507		
	Morose Nanook Table	507		
	Stake board	598		
	Brno Barcelona Chair	440		
5	Basket Ball	661	11981	625
	Rocking Horse	619		
	Antique Roman Vase	485		
	Magistoli Red	619		
	Tuscany	596		
6	Cappeline Embryo Chair	1056	18181	1424
	Goll ball_HI	1031		
	Kadesign m5_day	1051		
	Plane	1326		
	Zcol	1512		

Figure 3 above shows the secret models and the generated six shares along with the reconstructed secrets. It shows that the shares are unrecognizable and the secrets are reconstructed without loss; thus, the security criterion is satisfied. Similarly the other case is also tested using 2 secret 3D models, Pitcher and Bronto models for the scheme (3, 6), which suits the condition ($P\leq t$).The number of vertices present in these models is 12763 vertices and 29,974 faces. The prime number F_p chosen in this scheme is 12763.

Figure 4 above shows the two secrets and the generated shares for the case, where the number of secrets is less than the threshold. The secret is reconstructed without any loss. Various 3D models are tested for both the cases and can be compressed, using the Huffman coding and zlip as in [3]. Comparison between sizes of various 3D models and the generated shares for both the cases are given in Tables 1 and 2.

5. Conclusions and Future Work

The frame work proposed for multiple 3D models and its implementations and results are discussed in this paper. The proposed scheme makes use of the YCH algorithm for the secret sharing process. The verification property is implemented on both participants and the dealer, which identifies the duplicate share. The simulation results show that it is a perfect scheme and the feasibility is proved using different 3D models. Further, the size can be reduced by lossless compression techniques, such as the Huffman encoding and ZLIP.

References

[1] Blakley G., “Safeguarding Cryptographic Keys,” *in Proceedings of AFIPS National Computer Conference*, New York, USA, pp. 313-317, 1979.

[2] Chang C., Hsieh Y., and Lin C., “Sharing Secrets in Stego Images with Authentication,” *Pattern Recognition*, vol. 41, no. 10, pp. 3130-3137, 2008.

[3] Esam E. and Ben H., “Secret sharing Approaches for 3D Object Encryption,” *Expert Systems with Applications*, vol. 38, no. 11, pp. 13906-13911, 2011.

[4] Feng J., Wu H., Tsai C., Chang Y., and Chu Y., “Visual Secret Sharing For Multiple Secrets,” *Pattern Recognition*, vol. 41, no. 12, pp. 3572-3581, 2008.

[5] Guzin U., Mustafa U., and Vasif N., “Distortion Free Geometry Based Secret Image Sharing,” *Procedia Computer Science*, vol. 3, pp. 721-726, 2011.

[6] Khan B., Alghathbar K., Khan M., Alkelabi A., and Alajaji A., “Cyber Security Using Arabic CAPTCHA Scheme,” *the International Arab Journal of Information Technology*, vol. 10, no. 1, pp. 76-84, 2013.

[7] Lin C. and Tsai W., “Secret Image Sharing with Steganography and Authentication,” *Journal of Systems and Software*, vol. 73, no. 3, pp. 405-414, 2004.

[8] Lin S. and Lin J., “VCPSS: A Two-in-One Two Decoding-Options Image Sharing Method Combining Visual Cryptography (VC) and Polynomial-Style Sharing (PSS) Approaches,” *Pattern Recognation*, vol. 40, no. 12, pp. 3652-3666, 2007.

[9] Naor M. and Shamir A., “Visual Cryptography,” *in Proceedings of Workshop on the Theory and Application of Cryptographic Techniques Perugia*, Italy, pp. 1-12, 1995.

[10] Shamir A., “How to Share a Secret?,” *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, 1979.

[11] Shao J. and Cao Z., “A New Efficient (t, n) Verifiable Multi-Secret Sharing (VMSS) based on YCH Scheme,” *Applied Mathematics and Computation*, vol. 168, no. 1, pp. 135-140, 2005.

[12] Sorin I. and Ioana B., “Weighted Threshold Secret Sharing Based on the Chinese Remainder Theorem,” *Scientific Annals of Cuza University*, vol. 15, pp. 161-172, 2005.

[13] Thien C. and Lin J., “Secret Image Sharing,” *Computers and Graphics*, vol. 26, no. 1, pp. 765-770, 2002.

[14] Vikram J., Aparna M., Hariharan R., and Srinivasan E., “Number Theory Based Image Compression Encryption and Application to Image Multiplexing,” *in Proceedings of International Conference on Signal Processing, Communications and Networking*, Chennai, India, pp. 59-64, 2007.

[15] Wang R. and Su C., “Secret Image Sharing with smaller shadow images,” *Pattern Recognition Letters*, vol. 27, no. 6, pp. 551-555, 2006.

[16] Wen-Pinn F., “Non-Expansion Visual Secret Sharing in Reversible Style,” *IJCSNS International Journal of Computer Science and Network Security*, vol. 9, no. 2, pp. 204-208, 2009.

[17] Yang C., Chang T., and Hwang M., “A (t, n) Multi-Secret Sharing Scheme,” *Applied Mathematics and Computation*, vol. 151, no. 2, pp. 483-490, 2004.

[18] Zhao J., Zhang J., and Zhao.R., “A Practical Verifiable Multi-Secret Sharing Scheme,” *Computer Standards and Interfaces*, vol. 29, no. 1, pp. 138-141, 2007.

Jani AnbarasiL graduated from Manonmanium Sundaranar University, India in 2000 and received her MS degree in Anna University in 2005 in the field of computer science and engineering. At present she is a researcher in Anna University, India. Her research interests include cryptography, image processing and medical applications.

Anandha Mala received BE degree from Bharathidhasan University in Computer Science and Engineering in 1992, ME degree in University of Madras in 2001 and PhD degree from Anna University in 2007. Currently, she is working as Professor in Easwari Engineering College, Chennai, India, and heading the Department of Computer Science and Engineering. She has published more than 40 technical papers in various International Journal/ Conferences. She has 20 years of teaching experience on graduate level. Her area of interest includes image processing and grid computing.