Vizual kriptoqrafiya metodlarının icmalı

Səkinə Aydınova

Azərbaycan Respublikasının Prezidenti yanında Dövlət İdarəçilik Akademiyası

sekine_aydinova@yahoo.com

***Xülasə*— Texnologiyanın inkişafı ilə informasiya təhlükəsizliyi həyatımızda daha vacib rol oynayır. Dövrümüzdə informasiyanın virtual mühitdə bir yerdən başqa yerə çatdırılmasından çox təhlükəsiz şəkildə çatdırılması əhəmiyyət kəsb edir. Şəxsi məlumatların muhafizə edilməsi şəxsi təhlükəsizlik baxımından maddi və mənəvi itkilərin olmaması insanlar üçün vacibdir. Bu işdə informasiyanın virtual mühitdə təhlükəsiz ötürülməsini təmin edən vizual kriptoqrafik üsullar, vizual kriptoqrafiyanın tətbiq sahələri və əhəmiyyəti araşdırılmışdır.**

Açar sözlər—informasiya təhlükəsizliyi, vizual kriptoqrafiya.

I. GİRİŞ

İnformasiya təhlükəsizliyinin təmin edilməsi üçün bir çox kriptoqrafik yanaşmalar mövcuddur. Bu yanaşmalardan biri də vizual kriptoqrafiyadır. Vizual kriptoqrafiyada məxfi məlumatlar pay adlandırılan hissələrə bölünür və istifadəçilərə verilir, müəyyən sayda paylar birləşdirildikdə gizlədilən məlumatı əldə etmək mümkün olur.

Vizual kriptoqrafiyanın digər üsullardan əsas fərqi tətbiqinin asan olması və mühafizə edilən məlumatın bir neçə mərhələdən keçərək şifrlənməsi sayəsində daha təhlükəsiz olmasıdır.

Vizual kriptoqrafiya məxfi informasiya paylaşımı sxemlərinə əsaslanır. Vizual kriptoqrafiyada məxfi informasiya şəkillər vasitəsilə gizlədilir. Şəkillər bir neçə paya bölünməklə kodlaşdırılır. Kodların açılması şəklin hissələrinin "üst-üstə qoyulması" kimi sadə bir əməliyyatdır və heç bir hesablama tələb etmir. Vizual kriptografiya iki ideyanı: mükəmməl gizlilik və şifrlərin açılmasının çox sadə mexanizmini birləşdirir.

Vizual kriptoqrafiyanın bir çox tətbiq sahəsi vardır. Bunlara virtual mühitdə məlumtların təhlükəsiz şəkildə göndərilməsi, biometrik məlumatların gizliliyinin qorunması, biometrik autentifikasiya kimi tətbiqləri misal göstərmək olar.

Bu işdə vizual kriptoqrafiyanın yaranması, məxfi informasiya paylaşma sxemləri, vizual kriptoqrafiya üsulları və tətbiq sahələri araşdırlır.

II. MƏXFİ İNFORMASİYA PAYLAŞIMI SXEMLƏRİ

Məxfi informasiyanın paylaşılması dedikdə aşağıdakı sxem nəzərdə tutulur: məxfi informasiya bir qrup iştirakçı arasında paylaşılır, qrupdakı hər bir iştirakçıya həmin məxfi informasiyaın bir hissəsi verilir, bu hissələrin hər biri pay adlanır. Həmin paylar ayrılıqda istifadəyə yararsızdır. Məxfi informasiyaın aşkarlanması üçün yeganə yol kifayət sayda payın birləşdirilməsidir. Əgər bu paylar birləşdirilməsə (əlaqələndirilməsə) onların istifadəsi mümkün olmur və məxfi informasiya aşkarlana bilmir.

İlk məxfi informasiya paylaşma sxemi (secret sharing scheme, SSS) A. Şamir [1] və G. Blakley [2] tərəfindən kəşf olunmuşdur. Beləliklə, gizli paylaşma sxemində məxfi informasiya n sayda insan arasında paylaşılır. k sayda (və ya daha çox) insan paylarını əlaqələndirdikdə (burada $k \le n$) məxfi informasiyaı aşkarlamaq mümkün olur, əgər k-1 insan buna cəhd etsə, bu mümkün olmur. Buna əsaslanaraq, gizli paylaşma sxemini (k, n)-sxemi də adlanırırlar.

Adi Şamirin 1979-cu ildə nəşr edilən "Gizli informasiyanı necə paylaşaq" adlı məqaləsindən bir hissəyə baxaq [1]: "11 alim gizli bir layihə üzərində işləyir. Onlar bu layihədəki sənədləri kabinetdə gizli saxlamaq istəyirlər. Bu kabinet kilitlidir və yalnız və yalnız bu alimlərdən ən azı 6-sı eyni anda orada olarsa, kabinetin qapısını açmaq mümkün olmalıdır. Bu qapını açmaq üçün lazım olan ən az kilit sayı neçədir? Bu kilitləri açmaq üçün hər bir alim ən azı neçə açar daşımalıdır?

Minimal həll belədir: 462 kilit və hər bir alim üçün 252 açar. "

Həmin məqalədə A. Şamir, bu məsələyə əsaslanaraq (k, n) sxemini təklif edir. Həmin yanaşmanı belə izah etmək olar.

A. Şamir elementlərinin sayı kifayət qədər böyük olan sonlu meydan üzərində dərəcəsi k–1 olan çoxhədlidən istifadə etməyi təklif etmişdir. Məlumdur ki, dərəcəsi k–1 olan çoxhədlini onun k müxtəlif nöqtədəki qiymətlərinə görə birqiymətli bərpa etmək olar, ancaq bu zaman interpolyasiya üçün daha az sayda nöqtədən istifadə etmək olmaz.

Tutaq ki, n – iştirakçıların sayıdır, və məxfi s informasiyası n sayda $s_1, s_2, ..., s_n$ hissələrinə bölünüb. F sonlu meydanını seçək və onun 0-dan fərqli n müxtəlif $r_1, r_2, \ldots, r_n$ elementini götürək. Hər bir r_i elementini i-ci iştirakçıya uyğun qoyaq, i = 1, 2, ..., n. F meydanının k+1 sayda təsadüfi $a_0, a_1, \ldots, a_{k-1}$ elementlərini də seçək və onlardan F meydanı üzərində dərəcəsi k–1 olan $f(x)$ çoxhədlisini tərtib edək,

$$f(x) = \sum_{i=0}^{k-1} a_i x^i$$

$s=f(0)=a_0$ qəbul edək. $s_1=f(r_1)$, $s_2=f(r_2),\ldots$, $s_n=f(r_n)$ qiymətlərini sirrin hissələri kimi (r_i, s_i)) cütlərini iştirakçılar arasında paylayaq, i =1, 2, …, n. Bu sxemdə sirr $f(x)$ çoxhədlisinin sərbəst həddi a_0-dır.

s sirrinin bərpası üçün Laqranj interpolyasiya düsturundan istifadə edək. Tutaq ki, k sayda (x_i, $f(x_i)$) cütü var, burada $x_1, \ldots, x_t$ – F meydanının cüt-cüt müxtəlif elementləridir. Onda Laqranj düsturu aşağıdakı şəkildədir:

$$f(x)= \sum_{i=0}^{t} f(x_i) \cdot \prod_{j \neq i} \frac{x - x_j}{x_i - x_j}$$

$a_0=f(0)$ olduğu üçün Laqranj düsturundan alarıq:

$$a_0=\sum_{i=0}^{t} f(x_i)\cdot\prod_{j\neq i}\frac{x_j}{x_j-x_i}$$

Axırıncı düsturun köməyi ilə k iştirakçıdan ibarət istənilən qrup məxfi informasiyanı bərpa edə bilər. Eyni zamanda, bundan az sayda heç bir iştirakçı qrupu məxfi informasiyanı bərpa edə bilməz, çünki k–1 dərəcəli çoxhədlinin əmsallarını birqiymətli müəyyən etmək üçün meydanın k-dan az olmayan az sayda nöqtəsində çoxhədlinin qiyməti tələb olunur.

Karnin və yoldaşları [3] mükəmməl məxfi informasiya paylaşma (perfect secret sharing, PSS) sxemi anlayışını təklif etmişlər. Mükəmməl məxfi informasiya paylaşma sxemində informasiya paylanan şəxslər vacib və adi olaraq iki qrupa bölünür. Məxfi məlumatın vacib hissələri birinci qrup üzvləri arasında, vacib olmayan hissələri isə ikinci qrup üzvləri arasında paylaşılır. Bu üsulda yalnız birinci qrupdakı məlumaltlar birləşdirildikdə məxfi məlumatı əldə etmək olur.

PSS üslundan sonra meydana çıxan digər bir üsul adi qrupun böyüklüyü şərtində məxfi informasiyanın müəyyən sayda adi qrup üzvlərinə paylanması üsuludur. Bu üsul tənzimlənən məxfi informasiya paylaşma (ramp secret sharing, RSS) üsulu adlanır [4][5][6]. Daha sonra PSS və RSS üsulları da müxtəlif tədqiatçılar tərəfindən təkmilləşdirilmişdir [7][8] [9].

III. VİZUAL KRİPTOQRAFİYA

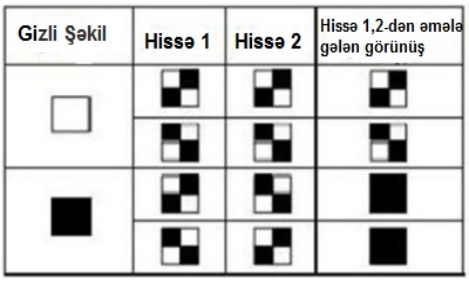
Vizual kriptoqrafiya məxfi informasiya paylaşma sxemləri əsasında Moni Naor və Adi Shamir tərəfindən kəşf olunmuş və 1994-cü ildə Eurocrypt konfransında açıqlanmışdır [10][11]: "Vizual kriptoqrafiya heç bir kriptoqrafik hesablama aparmadan sadəcə şəkilləri gizlədərək şifrələnən yeni tip kriptoqrafik sxemdir".

Naor və Shamir məxfi informasiya paylaşma anlayışını şəkil sahəsində təkmilləşdirmiş və vizual kriptoqrafiya adlandırmışlar. Şəkil paylaşma məxfi informasiya paylaşımının altçoxluğudur, çünki məxfi informasiya şəkillər vasitəsilə gizlədilir və bu ümumi məxfi paylanma probleminə xüsusi bir yanaşma tərzidir.

Şəkil paylama sxemi ümumi informasiyanın paylanmasına oxşarlığı müəyyən edir. (k,n) şəkil paylama sxemində məxfi informasiyanı hər biri pay adlanan n sayda hissəyə bölərək şəkil daşıyır və k sayda hissə olmasa və əlaqələndirilməsə açma funkisyası tamamilə uğursuz olur.

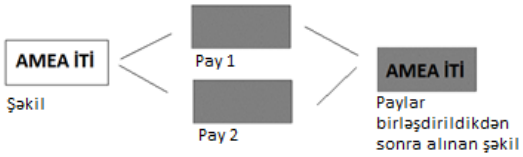
Noar və Shamirin 1994-cü ildə açıqıadıqları yeni üsul sadəcə binar şəkillərə tətbiq oluna bilir. Binar şəkil heç bir məna ifadə etməyən iki hissəyə ayırlır və bunlar paylaşılır [1]. Sonra bu iki məna ifadə etməyən binar şəkil bir yerə gətirildiyində isə ilkin binar şəkli verməlidir. Binar şəkil 0 və 1-dən əmələ gəlmiş bir şəkildir, yəni piksellər sadəcə ağ və qaradan ibarətdir.

Piksel parlaqlıq qiyməti sadəcə 2 sabit qiymətdən əmələ gələn binar şəkillər OR yada XOR üsulu ilə mənasız iki şəkilə ayrılır. Eyni şəkildə OR və XOR üsulları istifadə edilərək bu iki mənasız şəkildən ilkin binar şəkil əldə edilir.Aşağıda ağ və qara piksellərdən əmələ gəlmiş fərqli hissələr və bu hissələrin birləşməsindən əmələ gəlmiş ilkin piksellər göstərilmişdir. Qara rəngli pikseller hər halda əldə edilmiş ancaq ağ piksellər hər zaman əldə edilməmişdir.



Şəkil 1. Ağ və qara piksellərin paylanması və yenidən birləşdirilməsi

Aşağıdakı şəkildə isə bir şəkli binar formata çevirdikdən sonra iki hissəyə ayırma və təkrar birləşdirilməsi göstərilib (şəkil 2):



Şəkil 2.

Naor və Shamir ilkin olaraq fərz edirdi ki şəkil və ya mesaj ağ və qara piksellərdən ibarətdir, hər piksel fərdi idarə olunur və bu qeyd edilməlidir ki ağ piksel şəffaf rəngi göstərir. Buradakı bir mənfi cəhət budur ki açma funksiyası zamanı itki olur. Itki sahələri kontrastdır. Vizual kriptoqrafiyada kontrast çox vacibdir çünki insan vizual sistemi tərəfindən örtülmüş faylın aydınlığını o təyin edir. Nöqtələri və bu nöqtələr arasındakı məsafəni dəyişdirmək optik illuziya yaradır.

Verilən şəkil və ya yazı n hissə yaradılır və əgər onlardan k sayda hissə bir yerə gətirilibsə, ilkin şəkil (yazı) görünür. Əgər k hissədən azı birlikdədirsə şəkil gizli qalır. Hər piksel hər hissədə n şəkli dəyişmiş formada görünür. Paylar m qara piklsellər və ağ alt-piksellərin birlikdə yerləşməsinin toplamıdır. Struktur nxm ölçülü $S=(S_{ij})_{nxm}$ bul matrisi kimi təsvir oluna bilər: S_{ij}= 1 və ya 0 olur, yəni i nömrəli payın j nömrəli alt-pikseli ağ və ya qaradır.

Sxemin əsas parametrləri bunlardır:

1. M: bir paydakı piksellərin sayı. Bu ilkin şəkildən onu örtən şəkilə keçid zamanı itkini ifadə edir .
2. α : ilkin şəkildəki ağ və qara piksellərdən gələn əlaqələndirilmiş paylar arasındakı nisbi fərqi, kontrastdakı itkini ifadə edir.
3. γ : C_0 və C_1 toplusunun ölçüsü. C_0 ağ piksel üçün olan paylardakı alt-piksel nümunələrinə? C_1 isə qara piksel üçün olan paylardakı alt-piksel nümunələrinə istinad edir.

Payların konstruksiyası 2x2 vizual kriptoqrafiya sxeminə (VKS) görə çevrilə bilər. Ümumi halda, (2,2)-VKS 2x2 matrislərinin birləşməsi kimi müəyyən edilir:

C_0 = {Bütün matrislər $\begin{bmatrix}1&1&0&0\\1&1&0&0\end{bmatrix}$ matrisinin sütunlarının permutasiyasından əmələ gəlib}.

C_1 ={Bütün matrislər $\begin{bmatrix}1&1&0&0\\0&0&1&1\end{bmatrix}$ matrisinin sütunlarının permutasiyasından əmələ gəlib}.

Bu piksel genişlənmələrinə əsaslanaraq ilkin şəkildən bir piksel 4 piksellə yayılır. Paylar aşağıdakı qaydada yarana bilər:

1. Əgər ilkin binar şəklin pikseli ağdırsa, hər 2 pay üçün 4 pikselin eyni növləri təsadüfi yığılır.
2. Əgər ilkin binar şəklin pikseli qaradırsa, eyni sütundakı nümnuləri yığılır.

Paylar birləşdirilir və alt-piksellər düzgün sırada düzüləndə uyğunlaşdırılan qara piksellər paylar bul və ya sətirlər matrisi ilə ifadə olunur. Piksellər matrisin içinə müxtəlif yollarla yerləşdirilə bilər. Pay nümunələrinin müxtəlif tiplərinin vizual ifadəsi şəkil 3-də göstərilib.

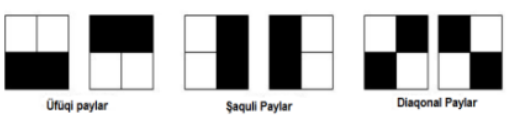
Şəkil 3

Vizual kriptoqrafiyanın məxfi informasiyaların təhlükəsiz şəkildə ötürülməsi, biometrik autentifikasiya, biometrik məlumatların gizliliyinin qorunması , çap və scan məxfiliyi kimi bir sıra praktiki tətbiqləri və bir çox üsulları vardır. Bunlardan bəzilərinə nəzər salaq:

IV. WU VƏ CHEN SXEMİ

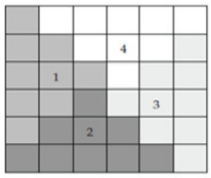
Wu və Chen 1998-ci ildə (2, 2)-lik yeni bir vizual məxfi informasiya paylaşma metodu təklif etdilər [12]. Bu metoda görə hər hansı iki gizli şəkil çevirmə üsulları istifadə edilərək iki pay içərisinə gizlədilə bilər. İstifadə olunan çevirmə bucaqları əksər hallarda 90, 180 və 270 dərəcə olmaqla yanaşı, paylar da kvadratik formaya malik olurlar. Kvadratik formada olmalarının səbəbi piksellərin bir-birini tam şəkildə örtməli olduğundandır.

2 *N*x*N* ölçülü şəkil 2*N*x2*N*-lik paylar əmələ gətirəcək şəkildə, hər piksel də 4 alt piksellə təmsil olunacaq şəkildə genişləndirilir. Bu 4 alt pikselə 2×2 lik genişləndirilmiş blok deyilir. Əmələ gətirilən bu paylar gizli şəkil haqqında heç bir məlumat verməz. Digər tərəfdən ilk gizli şəklin ələ edilməsi üçün piksellərin bir- birini tam örtüməsi şərtilə ilk iki pay üst üstə getirilərək əldə edilir. İkinci gizli şəklin əldə edilməsi üçün isə ilk pay 90° saat əqrəbi istiqamətinin tərsinə döndürülüb ikinci pay ilə üst üstə gətirildikdən sonra əldə edilir. Wu və Chenin alqoritminə görə ilk pay aşağıdaki kimi 4 bərabər üçbucaq formasında hissəyə ayrılır:



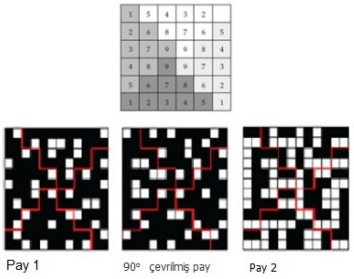
Şəkil 4.

İlk payın birinci hissəsində yerləşən hər bir 2×2 lik genişləndirilmiş bloklar aşağıdakı nümunələr (ing. pattern) çoxluğu içərisindən təsadüfi olaraq seçilməklə əldə edilir.



Şəkil 5.

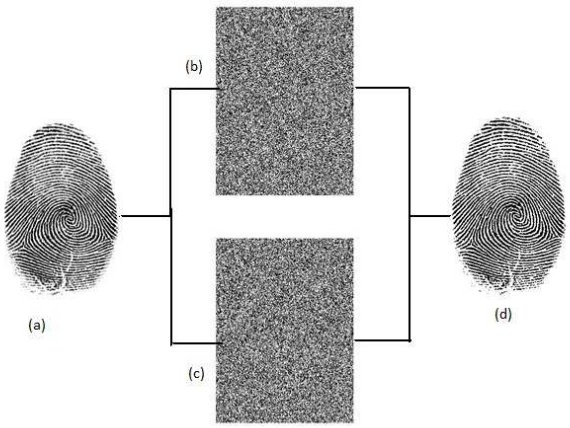
Digər 3 hissədəki nümunələrin seçilməsi prosesi də ilk hissə ilə eynidir. Wu və Chen ilk payı eyni tərkibə malik 4 üçbucaq formasında hisəəyə ayırır. Beləliklə hər bir hissə (NxN)/4 ədəd genişləndirilmiş bloka malik olur. Hər bir üçbucaq formalı hisəədə genişləndirilmiş bloklar eynidir. İlk hissədəki genişləndirilmiş bloklar təsadüfi seçilir və digər hissələrdə o nöqtəyə uyğun olan koordinata da eyni şəkildə köçürülür. Bu proses aşağıda göstərilmişdir.



Şəkil 6.

İkinci payın genişləndirilmiş blokları isə ilk payın genişləndirilmiş bloklarına, piksel rəng qiyməti isə gizli şəkil üzərindəki əlaqəli nöqtəyə əsasən təyin edilir.

Məxfi informasiyaların ötürülməsi ilə yanaşı biometrik gizliliyin qorunması sahəsində dahaq dəqiq desək barmaq izinin qorunmasında bu üsula üstünlük verilir.



Şəkil 7. (a) İlkin barmaq izi şəkli; (b) Pay 1; (c) Pay 2; (d) Payların birləşdirilməsi ilə alınan ilkin şəkil.

V. THİEN VƏ LİN SXEMİ

Thien ve Lin, Shamir tərəfindən 1979-cu ildə verilən gizli paylaşma sxemini isitifadə edərək (*k*, *n*) əsaslı bir şəkil paylaşma üsulu təqdim etmişdirlər [13] [14].

Üsulun əsas ideyası $l \times l$ ölçülü gizli şəkildən *n* ədəd pay-şəkil əldə etmək üçün (k-1) dərəcəli bir polynomial funksiya istifadə olunmasıdır.

$0 \le i \le \frac{l}{k}$ və $1 \le j \le l$ şərtələri daxilində polynomial funksiya bu şəkildə ifadə olunur:

$$S_x(i, j) = I(ik+1, j) + I(ik+2, j)x + ... + I(ik+k, j)x^{k-1} (\text{mod } p)$$

Bu metod vasitəsilə alınan şəkillərin ölçüsü ilkin şəklin ölçüsündən $\frac{1}{k}$ dəfə böyükdür.

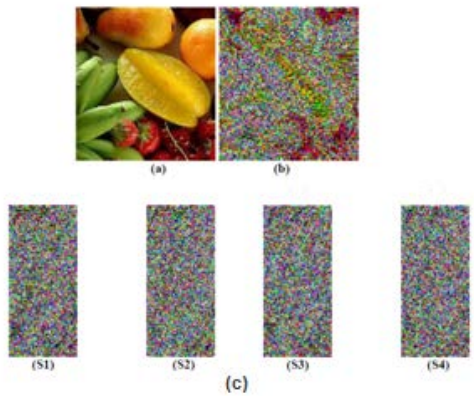
Əldə edilən şəkil hissələri - paylar iştirakçılara göndərilir. Ən azı *k* sayda iştirakçı bir yerə gələrək ilkin şəkli əldə edə bilir. Bunun üçün Laqranj interpolyasiya üsulu istifadə olunur. Laqranj İnterpolyasiya üsulu aşağıdakı şəklidə göstərilib:

$$h(x) = \sum_{k=1}^{s} y_k \prod_{\substack{j=1 \\ j=k}}^{s} \frac{x - x_j}{x_k - x_j} \ (mod\ p)$$

Düsturdakı *k*, iştirakçıların sayını, *y* şəkil paylarındakı rəng qiymətlərini göstərir. Burada bölmə əməliyyatı üçün istifadə edilən *mod* toplama əməliyyatı üçün də istifadə olunur.

Thien və Lin bu metodla əlavə olaraq iştirakçılara paylaşma əməliyyatından əvvəl şəklin permutasiya edilməsini də tövsiyyə edir. Permutasiya əməliyyatı hər hansı bir açar qiyməti ilə edilə bilər. Permutasiya əməliyyatı təhlükəsizliyi və hücumlara qarşı müqavimətin artırılmasını təmin edir.

Thien və Linin göstərdiyi bu üsul Naor və Shamirin üsulundan fərqli olaraq rəngli şəkillərə də tətbiq oluna bilir.



Şəkil 8. (a) Seçilən nümunə şəkil; (b) permutasiya edilmiş şəkil; (c) əldə edilmiş paylar.

NƏTİCƏ

Daim inkişaf edən texnologiyalar həyatımızı asanlaşdırsa da, fərdi və məxfi məlumatların mühafizəsi çətin bir problemə çevrilir. İnternetin yayılması ilə artan informasiya mübadiləsi və paylaşımı nəticəsində mətn, səs və şəkil kimi bir çox informasiyanı özündə saxlayan fayllar dünyanın müxtəlif yerlərindəki insanlar tərəfindən paylaşıla bilir.

Məxfi informasiyanı qorumaq üçün müxtəlif üsullardan istifadə olunur. Bu işdə məxfi informasiyanı mühafizə etmək üçün vizual kriptoqrafiya üsulları tədqiq edilmişdir.

Alınan nəticəyə əsasən vizual kriptoqrafiya tətbiqi asan, mühafizəsi güclü məxfi informasiya paylaşma üsuludur. Binar və rəngli şəkillərə tətbiq oluna bilir, bu isə onu istənilən sahədə istifadə edilməsinin mümkün olduğunu göstərir. Gələcək məqsəd isə burada göstərilən üsulları təkmilləşdirərək və ya bir neçə üsulu birləşdirərək yeni bir vizual kriptoqrafiya üsulu yaradaraq məxfi məlumatların mühafizəsini daha yüksək səviyyəyə çıxarmaqdır.

ƏDƏBİYYAT

[1] A. Shamir, “How to share a secret,” Communacations of the ACM, vol. 22, No. 11, pp. 612-613, 1979.

[2] G. R. Blakley, “Safeguarding cryptographic keys,” Proc. of AFIPS National Computer Conference, vol. 48, 4–7 June 1979. p. 313–317.

[3] E. D. Karnin, J. W. Greene, M. E.Hellman, “On secret sharing systems,” IEEE Transactions on Information Theory, vol.IT-29, no. 1, pp. 35–41, Jan. 1983.

[4] K. Kurosawa, K. Okada, K. Sakano, W.Ogata, and S. Tsujii, “Nonperfect secret sharing schemes and matroids,” Lecture Notes in Computer Science, vol. 765, pp.126–141, 1994.

[5] W. Ogata and K. Kurosawa,”Some basicproperties of general nonperfect secret sharing schemes” Journal of Universal Computer Science, vol. 4,no. 8,pp. 690–704, 1998.

[6] P. Paillier, “On ideal non-perfect secret sharing schemes,” Proc. of the 5th International Workshop on Security Protocols, 1997, pp. 207–216.

[7] C. Asmuth, J. Bloom, “A modular approach to key safeguarding,” IEEE Transactions on Information Theory, vol. 29, no.2, pp. 208–210, 1983.

[8] G. R. Blakley, C. Meadows, “Security of ramp schemes,” Advances in Cryptology – Crypto ’84, Aug.1984, pp. 242-268.

[9] A. De Santis, B. Masucci, “Multiple ramp schemes,” IEEE Transactions on Information Theory, vol. 45, no. 5, pp. 1720–1728, July 1999.

[10] M. Naor, A. Shamir, “Visual cryptography,” Proceedings of the Conference on Advances in Cryptology – Eurocrypt’94, 1994, pp. 1–12.

[11] M. Naor, A. Shamir, “Visual cryptography II: Improving the contrast via the cover base,” Proceedings of the International Workshop on Security Protocols, 1996, pp. 197-202.

[12] H. Chen, C.C. Wu, “A Study on Visual Cryptography,” Master thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C.,1998.

[13] C.-C. Thien, J.-C. Lin, “Secret image sharing,” Computers & Graphics, vol. 26, no. 5, pp. 765–770, 2002.

[14] B. Lee, “A reliable (k, n) image secret sharing scheme”, Proceedings of the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing, 2006, pp. 31-36.