Blakley'in Gizli Sır Paylaşımına dayalı DataMatrix ECC200 Kodlama

Vasif Nabiyev[1] Katira Soleyman zadeh[2]

[1,2]Department of Computer Engineering, Karadeniz Technical University, Trabzon 61080, Turkey

[1] e-posta: vasif@ktu.edu.tr [2]e-posta: katirasole@gmail.com

Özetçe

Barkodlar, ticari ürünlerle birlikte, sağlık sistemi, askeri belgeler ve hassas iş verileri gibi sayısız uygulamalarda kullanılmaktadır. Bu bilgilerin çoğu gizli ve güvenli tutulmalıdır. Ancak barkodun içeriği doğrudan mobil cihazlar tarafından okunabilir. Makalede verilerin güvenliğinin artırılması için DataMatrix ECC200 kodu ile gizli paylaşıma dayalı şema önerilmektedir. Korumalı veri paylaşımı Blakley'in gizli paylaşım şemasına dayalı olarak gerçekleştirilmiştir. Önerilen bu şema içerisinde gizli veri paylara ayrılır ve sonra pay bilgileri DataMatrix etiketleri içerisine gömülür. Önerilen şema veri iletiminde güvenliği artırmaktadır.

1. Giriş

Barkodlar geleneksel sembol açısından anahtar alfanümerik bilgileri kodlamak için kullanılır ve sayısal sistemler bilgileri tarayarak okumaktadır. 1D ve 2D barkodların farklı türleri Tablo-1'de gösterilmiştir. Sayısal verinin kodlanması, tek-boyutlu (1D) barkodlar, ürün sevkıyat ve izleme, sistem güvenliği, süpermarketler vb gibi uygulamalar son iki yılda önemli bir rol oynamaktadır [1,2,3,4]. 2D barkod ile veri hem yatay hemde dikey yönde kodlanır. 2D sembolünde veri miktarı önemli ölçüde 1D sembolünde depolanandan daha büyüktür. 2D barkod çözümleri, özellikle açık olarak bilgi kodlama yerine basit bir kod bilgisi gerektiren uygulamalar için, geleneksel 1D barkodlarına göre daha fazla bilgi yoğunluğu sağlar. 2D barkod teknolojisinin birkaç uygulamaları, ürün etiketleme, izleme ve kontrol, mobil güvenlik, göç çek hizmetleri, sağlık hizmetleri, e-ticaret vb. dir. 2D barkodları üzerinde depolanan ürün açıklamalarını insanlar mobil cihazlar yardımıyla kolayca okuyabilirler. Bu gizli olması istenen veriler için de geçerlidir. Bu nedenle, verilerin güvenli şekilde korunması çok önemlidir. Gizli paylaşım, bu sorunu çözmek için sunulmuştur. Çalışmada, paylar için Blakley sır paylaşımı yöntemi ile oluşturulan veriler DataMatrix kodları içerisine gömülerek sistemin güvenirliği artırılmıştır [5,6,7].

1.1. Sır Paylaşımı

Gizli paylaşım şemaları, verinin iletiminde tek bir kişiye güvenmeden gerçekleştirilen uygulamalarda kullanılmaktadır. Gizli paylaşım şeması verilerin bütünlüğünün korunmasında güvenli bir yöntemdir. Bu şemada gizli bilgiyi ileten bir dağıtıcı ve sonlu sayıda katılımcılar $P=\{p_1,\ldots,p_n\}$ bulunmaktadır. d verisi n parçalara ayrılır $d_1,\ldots,d_n$ ve her d_i payı ilgili katılımcılar p_i ($1 \le i \le n$) arasında dağıtılır. Bunun sonucunda, paylaşılan veri, veri bozulması ve kaybı sorununu azaltmak için ayrı ayrı paylarda saklanabilir. Gizli paylaşım şemasında:

1) eğer $P' = \{p_{i_1},\ldots, p_{i_l}\} \subset P$ yetkili pay kümesiyse, gizli veri elde edilmektedir.

2) eğer $P' = \{p_{i_1},\ldots, p_{i_l}\} \subset P$ yetkisiz pay kümesiyse, o zaman gizli veri bu paylardan yeniden elde edilmemektedir.

1979 yılında, Shamir ve Blakley ilk (k,n) eşik gizli paylaşım yöntemini önerdiler[8,9,10]. Bu şemalar sırasıyla, Lagrange polinomial interpolasyon ve afin hiperdüzlemlere dayanmaktadır. Makalede, Blakley yöntemine dayalı gizli bir paylaşım yöntemi önermektedir.

Tablo1: 1D Barkodları ve 2D Barkodlar

1D barcodes	2D barcodes
Codabar 	Maxicode 
Extended Code 39 	DataMatrix 
EAN bookland 	Aztec Code 
UPC-A 	QR Code 

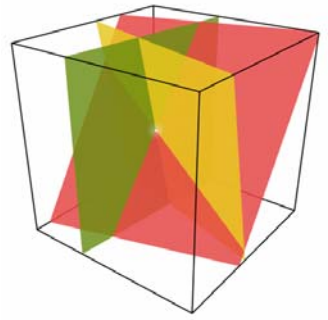
1.2. Blakley gizli paylaşım şeması

Blakely şeması, altdüzlem geometriye dayalıdır [11,12]. T boyutlu uzayda bir nokta sır olarak alınır ve paylar, bu nokta üzerinden geçen bir afin altdüzlemidir.

Afin altdüzlemi lineer denklem tarafından gösterilmektedir.

$$a_1 x_1 + \ldots + a_t x_t = b$$

T hiperdüzlemler alındığında, gizli nokta, bu t hiperdüzlemlerin kesişme noktasında yer alır. Şekil 1'de üç hiperdüzlemin sadece bir noktada (gizli noktası) nasıl kesiştiği gösterilmiştir.



Şekil 1: Gizli nokta üç düzlem arasındaki kesişme noktasında[12]

1.3. DataMatrix

Genel olarak, 2D barkodlarının iki türü vardır: PDF417 ve Kod 49 gibi yığılmış 2D barkod, QR kod ve DataMatrix gibi matrisli barkod. Makalede DataMatrix barkod teknolojisi kullanılmaktadır.DataMatrix barkodların CRC ve konvolüsyon hata düzeltme ve Reed-Solomon(RS) hata düzeltme tekniği olmak üzere iki versiyonu vardır. ECC200 Reed-Solomon hata düzeltmeli DataMatrix'ler yeni uygulamalar için tavsiye edilir [13,14,15]. 2D DataMatrix barkodu, MxN boyutlu bir görüntüdür. DataMatrix kare veya dikdörtgen yapılı bir semboldür. DataMatrix, daha fazla veri içermek için, hizalama şablonuyla ayrılmış ve böylece birden fazla veri bölgeleri sağlamaktadır. Veri bölgesi, bir vizör şablonu ile çevrilidir. DataMatrix barkod, barkodun %60'ı bulanık olsa bile çözülebilmektedir (barkod boyutuna bağlıdır) [16].
DataMatrix özellikleri kısaca aşağıda verilmiştir:

- Yüksek veri kapasitesi: Tek bir DataMatrix sembolü teorik olarak 3116 rakam, 2335 alfanümerik karakterleri veya 1556 byte tutabilir.
- Varsayılan karakter seti Latin-1 veya ANSI ASCII dir.
- Data Matrix baskı kalitesi: DataMatrix barkodunun kalitesini optimize etmek için 4 ila 5 pikselden daha küçük nokta ile basılmamaktadır.
- Veri Temsilciliği: 1 değeri için siyah piksel, 0 değeri için ise beyaz piksel kullanılır.
- Seçilebilir hata düzeltme tekniği:
  ECC 200: Reed-Solomon hata düzeltme.
  ECC 000 - 140: Konvolüsyonel hata düzeltme,
- Kodunu türü: Matrix
- Oryantasyon bağımsızlık: vardır

2. Önerilen Yöntem

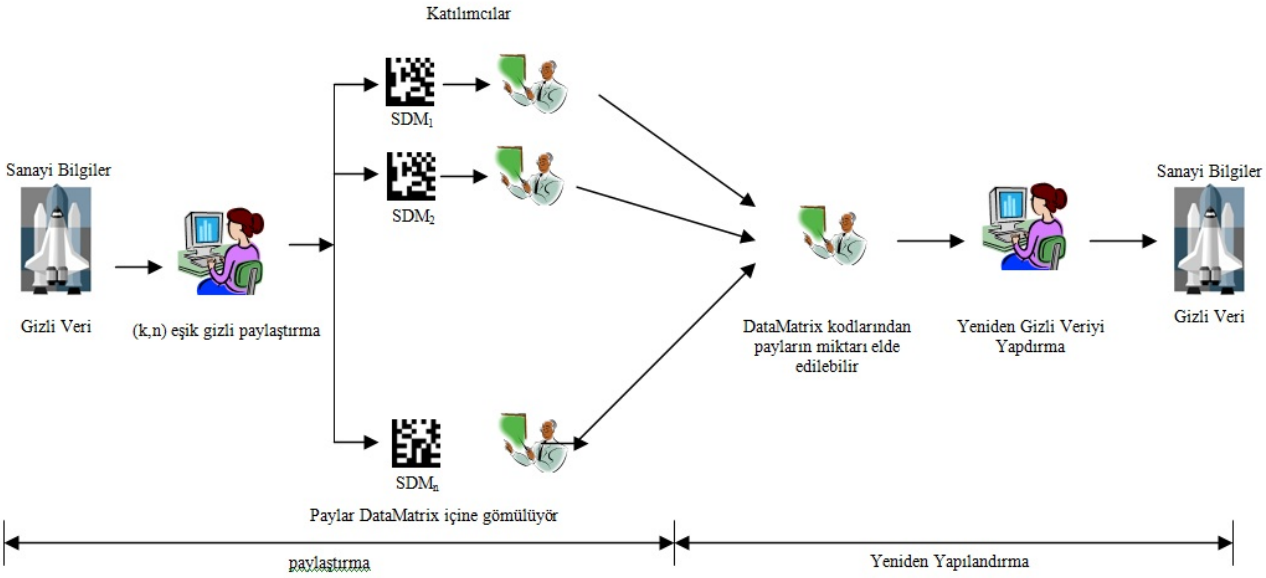
Önerilen yöntemde DataMatrix barkodların veri güvenliğini artırmak için, bir gizli paylaşım tekniği tasarlanmaktadır. Bu yöntemde, Blakley'in şeması aracılığıyla gizli veri paylara ayrılır ve her pay, bir DataMatrix taşıyıcı içine gömülür. Bu paylar katılımcılar arasında dağıtılır. Katılımcıların herhangi birisi kendi DataMatrix'inden gizli veriye ulaşmak isterse, ortaya çıkan veri anlamsız olacaktır. Gizli veri, sadece pay sayısı önceden tanımlanmış bir eşik değere eşit veya daha büyük olduğu zaman elde edilebilir.

2.1. Paylaştırma Algoritması

Önerilen şemada gizli veri, x dizisi için $x=(x_1,\ldots, x_n)$ aşağıdaki şekilde n hiperdüzlemlere ayrılacaktır.

$$a_1x_1+\ldots+a_nx_n=b \qquad (1)$$

Gizli veri, (k,n) eşik şemasına göre herhangi k ($k \leq n$) yada daha fazla hiperdüzlemlerin kesişme noktasını bularak, elde edilebilir. Şekil 2, sistemin genel yapısını göstermektedir.



Şekil 2: Sistemin genel şeması

Paylaşım algoritması aşağıdaki adımları içermektedir:
Adım 1: (k, n) eşik şeması seçilir.
Adım 2: Gizli veri, k karakterli örtüşmeyen kümeler haline bölünür.
Adım 3: Her bir k karakter için
3.1. k karakter değerleri (ASCII değeri) alınır
3.2. Rastgele n farklı çözüm seti ($a_1,a_2,\ldots,a_k$) seçilir ve n pay değerlerini üretmek için denklem 1'e koyulur.
Adım 4: Her bir pay DataMatrix içerisine gömülür.

2.2. Yeniden Yapılandırma Algoritması

Yeniden yapılandırma algoritması (k, n) eşik şemasına göre k veya daha fazla DataMatrix barkodlarından gizli veriyi yeniden hesaplamaktadır. Herhangi bir DataMatrix barkodlardan gizli veri kesinlikle elde edilemez, bu barkodlarda yalnız anlaşılamayan pay bilgileri bulunmaktadır. Yeniden yapılandırma algoritması aşağıda verilmiştir.
Adım 1: (k,n) aynı eşik şeması kullanılır ve k veya daha fazla DataMatrix barkod seçilir.
Adım 2: k adet DataMatrix barkodlarının bilgileri yeniden elde edilir.
Adım 3: Elde edilen bilgiler denklem 1'e koyulur ve x dizisi hesaplanır. Sonuçta gizli veri tekrar elde edilir.

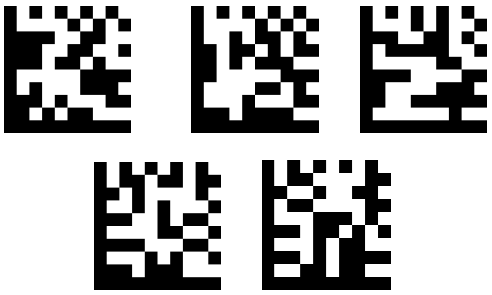
Örnek olarak "SECRETEST" kelimesini ele alalım. Önce kelime Blakley gizli paylaşım şemasıyla k paya bölünür, sonra ise DataMatrix kodlarına gömülür. (3,5) eşik gizli paylaşımı kullanılarak "SEC" karakterleri "-=h" karakterlerine denk gelecek. Bu karakterlere karşı düşen ASCII değerler sırasıyla (45, 61, 104)'dür. Bu değerler aşağıdaki bağıntıya göre kelime koduna çevrilir:

Kelime_kodu=(karakterlerin sayısal miktarı) +1

Reed-Solomon hata düzeltme tekniği kullanılır ve 5 tane hata düzeltme kelime kodu oluşturulur ve sonra her bir sayı ikili hale çevrilir. İkili sayılar DataMatrix barkodlarını oluşturmaktadır. Sonuçta parçalanmış bilgiler birleştirilerek başlangıç veriler güvenli şekilde tekrar elde edilir.

3. Deneysel Sonuçlar

Son zamanlarda ürün hakkındaki bilgiler ve özellikler, DataMatrix barkodlarına taşınmaktadır. Ancak doğrudan Datamatrix kod içeriğinin okunması mümkündür. Önerilen şema DataMatrix kodlarının gizli verilerinin güvenliğini artırmaktadır. Gizli veri Blakley gizli paylaşım teknikleri ile paylara bölünür ve sonra DataMatrix kodlarının içerisine gömülür. Katılımcılar ayrılıkta kendi payından gizli veriyi elde edememektedir. Pay sayısı önceden tanımlanmış bir eşik değerine eşit veya daha büyük olduğu halde gizli veriler tekrar elde edilmektedir. Bu şemada veriler doğrudan DataMatrix içerisine gömülmektedir ve bu nedenle DataMatrix barkodların verilerini aramak için ayrıca bir veritabanı olmasına gerek olmamaktadır. Önerilen çalışmada pay boyutu, gizli verinin sadece dörtte biridir, böylece sistem maliyeti çok daha düşüktür ve Datamatrix içerisine daha çok gizli veri kodlanabilir. DataMatrix barkod kısmen hasarlı olsa bile okunabilir.
Şekil 3'te (3,5) eşik gizli paylaş şeması örneği verilmiştir. İlk olarak, gizli veri Blakley gizli paylaşım tekniği ile paylara bölünür. Sonra üretilen paylar her DataMatrix kodları içerisine kodlanır. (3,5) eşik gizli paylaşım şemasında alınan Datamatrix kodlarının sayısı üçe eşit veya daha büyük olması durumunda, gizli veri elde edilmektedir. Yeniden yapılandırma aşamasında, herhangi üç pay ve ya üçten büyük pay alınırsa gizli veri tekrar elde edilebilir.



Şekil 3: "SECRETEST" kelimesini içeren DataMatrix barkod görüntüleri

4. Değerlendirme

Bu çalışma, DataMatrix kodlarındaki verinin güvenliğini artırmak için bir yöntem sunmaktadır. Önerilen teknik, ilk gizli veriyi Blakley gizli paylaşım yöntemi ile paylara ayırır ve paylaşılan veriler daha sonra doğrudan DataMatrix etiketleri içerisine gömülür. Böylece herkes doğrudan DataMatrix içeriğini okuyamamaktadır. Veri kaybını önlemek için barkod %60 bulanık olsa bile, Reed-Solomon algoritmasına dayalı hata düzeltme kod kelimeleri ile çözülmektedir. Önerilen teknik, tıbbi e-sağlık sistemi, askeri belgeler, ticari işlemler, elektronik bilet, posta hizmetleri ve diğerleri gibi bazı uygulamalarda kullanılabilir.

5. Kaynakça

[1] ISO/IEC16022, "Information technology-Automatic identification and data capture techniques-Data Matrix barcode symbology specification"
[2] NATO Standard Barcode Handbook, AAP-44(A), September 2010.
[3] National Aeronautics and Space Administration," Application of Datamatrix identification symbols to Aerospace parts using direct part marking methods/techniques", NASA-HDBK-6003C,2008.
[4] M.Krasikov, "DataMatrix barcode search algorithm on post envelope and decoding program development", Information Technology, Management and Society, Volume 2, No.1, 13-22, ,2009.
[5] Tso, H.-K., "Sharing secret images using Blakley's concept", Optical Engineering, vol. 47, no. 7, 2008.
[6] C.C. Thien and J.C. Lin, "Secret image sharing," Comput. Graph. 26, 765–770, 2002.
[7] 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, 2010.
[8] Blakley,G.R., "Safeguarding Cryptographic Keys", Proceedings of the National Computer Conference, pp. 313-317, 1979.
[9] A. Shamir, "How to share a secret," Communications of the ACM, Vol. 22, pp. 612-613, 1979.
[10] M.Naor and A.Shamir,"Visual cryptography," in Proceedings of Advances in Cryptology-EURPOCRYPT, LNCS 950, pp. 112, , 1995.
[11] Chen, C.-C., Fu, W.-Y, "A Geometry Based Secret Image Sharing Approach", Journal of Information Science and Engineering, Vol 24, No.5, pp. 1567-1577, 2008.
[12] Esam Elsheh1 and A. Ben Hamza2," SECRET SHARING OF 3D MODELS USING BLAKELY SCHEME", 25th Biennial Symposium on Communications, IEEE, pp.92-95, 2010.
[13] Jie Gao," Reed Solomon Code", February 19, 2007.
[14] C.K.P. Clarke,"Reed Solomom Error Correction", BBC R&D white Paper, WHP 031, july 2002.
[15] Jasmin Oz and Assaf Naor," Reed Solomon Encoder/Decoder on the StarCore™ SC140/SC1400 Cores, With Extended Examples", Freescale Semiconductor Inc., Document Order No. AN2407, Rev.1 ,12/2004.
[16] GSI DataMatrix, www.gs1.org,2010