GÜVENLİ İLETİŞİM İÇİN YENİ BİR VERİ GİZLEME ALGORİTMASI

Ali DURDU[1] ve Ahmet Turan ÖZCERİT[2]
[1]Sakarya Üniversitesi, Mühendislik Fakültesi, Yazılım Mühendisliği Bölümü, Sakarya
[2]Sakarya Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Sakarya

adurdu@sakarya.edu.tr, aozcerit@sakarya.edu.tr

ÖZET

Bu çalışmada, güvenli iletişim için kullanılacak imgeler için yeni bir veri gizleme yöntemi önerilmiştir. Önerilen sırörtme yöntemi sıkça kullanılan yer değiştirme yöntemi yerine eşleştirme yöntemini kullanmaktadır. Önerilen yöntemde veriler sıralı olarak gizlenmektedir. Yöntemin başarım performansı literatürdeki çalışmalar ile kıyaslanmış ve sonuçlar gösterilmiştir. Bu makale, ISDFS 2015'de sunulmuş ve seçilerek bu dergimizde basılmıştır.

Anahtar Kelimeler: steganografi, steganaliz, veri gizleme, güvenlik, iletişim

A NEW APPROACH FOR DATA HIDDEN METHOD BASED ON STEGANOGRAPHY

ABSTRACT

This work proposes a novel data hidden method for secure communication. Proposed data hidden method use least-significant-bit (LSB) matching instead of LSB. The new method modified one bit for four bits. Therefore, the method allows embedding same data as LSB but fewer changes. The experimental results of the proposed method show better performance than other exist literature works and LSB.

Keywords: steganography, steganalysis, daha hidden, secure communication

I. GİRİŞ (INTRODUCTION)

İnternet teknolojilerinin gün geçtikçe gelişmesi ve hızlı bir şekilde hayatımıza girmesiyle birlikte iletişim olanakları son derece artmıştır. Anlık olarak sürekli hızlı iletişim ortamlarının en büyük sorunu güvenlik olmuştur. İletişimde güvenlik unsuru üzerinde çalışan birçok çalışma vardır. Şifreleme veya sırörtme (steganography) yöntemleri bunlar arasında sayılabilir.

Şifreleme günümüzde de sıkça kullanılan bir güvenlik yöntemidir. Şifrelemede iletilecek veri iletim ortamında üçüncü kişilerin anlayamayacağı şekilde şifreleme algoritmasına bağlı olarak kodlanır. Şifreleme algoritmalarının bulunması ile şifre çözme algoritmaları bulunmuş ve böylece birbirini sürekli geliştiren bir süreç başlamıştır. Şifreleme yönteminde en büyük açık gönderilen verinin anlamsızlığı nedeniyle şifreli olduğunun bilinmesi ve içerdiği bilginin önem taşıdığının anlaşılmasıdır. Bu nedenle şifreli veri çözülemese de iletişimin engellenebilmesi için iletim hattına saldırılarda bulunulabilir. Veri iletişiminin engellenmesi, şifreleme işlemini geçersiz ve yararsız kılacaktır.

Sırörtme de iletilen gizli veri açık bir şekilde sergilenmez. Gizli veri fark edilmeyecek bir ortamda

gizli bir şekilde saklanır. İletilecek gizli veri herhangi bir dosyaya gömülerek masum bir şekilde transfer edilebilir. Sırörtmede iletilecek veri, ayrıca şifreleme mekanizmaları ile de desteklenerek iki boyutlu bir güvenlik sistemi oluşturulabilir. Sırörtme yöntemlerine karşı da geliştirilmiş bazı saldırı yöntemleri mevcuttur. Sıraçma olarak isimlendirilen bu yöntemler, örtü dosya içerisindeki gizli verinin algılanmasını amaçlayan birçok farklı mekanizmalar içerebilir. Yapılan çalışmalarda, sayısal ortamda sırörtme yöntemleri genellikle resim dosyaları üzerinde uygulanmıştır [1,5]. Resim dosyalarından farklı olarak hareketli görüntüler üzerinde çalışan Çetin ve Özcerit video dosyalarının içerisine gizleme yapacak renk histogramına dayalı yeni bir gizleme tekniği sunmuşlardır [6].

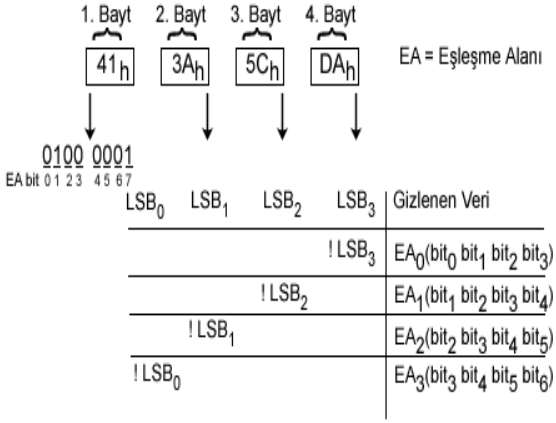
Bu çalışmada, imgeler için yeni bir veri gizleme yöntemi sunulmuştur. Önerilen yöntemin başarımı literatürdeki çalışmalarla kıyaslanmıştır. Bölüm 2'de önerilen yöntem, Bölüm 3'de ise önerilen yöntemin başarım performansı verilmektedir. Çalışmanın sonucu ise Bölüm IV'de verilmiştir.

II. ÖNERİLEN VERİ GİZLEME YÖNTEMİ

Eşleşme alanı mantığına göre çalışan veri gizleme yöntemlerinde amaç gizlenecek bilgiyi varolan bitleri değiştirmeden kullanarak gizlemek ve imgede mümkün olabilecek enaz değişiklikle veri gizleme işlemini tamamlamaktır. Geleneksel yer değiştirme yönteminde (LSB) ise gizlenecek verilerin bitleri parça parça imgenin her bir baytının son bitine saklanır. Burada son bitler 1 yada 0 olarak değiştirilmektedir. Burada iki durum söz konusu olduğu için imgenin son bitleri %50 oranında değişime uğramaktadır. Yani 1000 bit veri gizlendiğinde ortalama olarak örtü imgede 500 bitlik bir veri değişmiş olur.

Eşleştirme yönteminde ise dosyanın son bitleri doğrudan değiştirilmez. Bunun yerine imgedeki bitler korunarak gizlenmek istenen bilgi varolan bitler ile temsil edilmeye çalışılır. Buda imgede en az değişiklik oluşturduğu için gizleme işlemin ortaya çıkma ihtimalini azaltır.

Önerilen yöntemde örtü imgesi 4 baytlık çerçevelere bölünür. 1. baytın baştan(MSB) 7 biti eşleştirme alanları için kullanılır. 7 bitlik bilgiden 4 adet eşleştirme alanı oluşturulur. Buna göre bit_0, bit_1, bit_2 ve bit_3 EA_0 olarak adlandırılmıştır. 4 bit sağa kaydırma (shift) yöntemi ile bit_1, bit_2, bit_3 ve bit_4 EA_1, bit_2, bit_3, bit_4 ve bit_5 EA_2 ve bit_3, bit_4, bit_5 ve bit_6 EA_3 olacak şekilde 4 farklı eşleşme alanı oluşturulmuştur. Bu 4 bitlik eşleşme alanlarına uygun olarak gizlenecek mesajda 4-bit gruplar halinde bölünür. İlk 4 bit ile işleme başlanır ve eşleşme alanlarından birisine eşit olup olmadığına bakılır. Eğer eşleşme alanlarından hiçbirisine eşit değilse bir sonraki 4 baytlık çerçeveye geçilir. 4 bitlik mesajın bu çerçeve için eşleşme alanlarından birine eşitliği araştırılır. Eşleşme alanlarından birisine eşitse Şekil 1'deki tabloda gösterildiği gibi ilgili baytın son biti (LSB) terslenir. Örneğin EA_3 eşleşme alanına eşit ise 1. baytın son biti terslenir. Böylece çerçevede bilginin hangi bitlerde olduğu işaretlenmiş olur. LSB bitlerine veri gizleneceği için eşleşme alanı bitlerine dahil edilmez.



Şekil 1. Önerilen gizleme yöntemi çalışma mantığı

```
function embedded_method1(C,M)
    max_block_size=sizeof(C)/4
    message_size=sizeof(M)
    i=1
    while i<=max_block_size
        if i>=message_size then
            exit while
        end if
        if say=1 then
            message_piece=M(i,1:4)
            say=2;
        else
            message_piece=M(i,5:8)
            say=1;
        end if
        if  C(i,1:4) = message_piece then
            C(i,8)= Not C(i,8)
        else if C(i,2:5) = message_piece then
                C(i+1,8)= Not C(i+1,8)
            else if C(i,3:6) = message_piece then
                    C(i+2,8)= Not C(i+2,8)
                else if C(i,4:7) = message_piece then
                        C(i+3,8)= Not C(i+3,8)
                    end if
                end if
            end if
        end if
        i=i+4
    end while
end function
```

Şekil 2. Önerilen gizleme yöntemi için sözde kod.

Şekil 2'de önerilen gizleme yöntemi 1'in sözde kodu verilmiştir. Şekil 2'de gösterilen kısaltmaların anlamları aşağıda verilmiştir.

- Cover imgenin i. pozisyondaki baytın değerini C(i)
- Cover imgenin i. pozisyondaki baytın değerinin ilk 4 biti C(i,1:4)
- Cover imgenin i. pozisyondaki baytın değerinin ilk 4 bitinden itibaren 1 bit sağa kaydırma sonucu C(i,2:5)

- Cover imgenin i. pozisyondaki baytın değerinin en önemsiz biti (LSB) C(i,8)
- Cover imgenin i+1. pozisyondaki baytın değerinin en önemsiz biti (LSB) C(i+1,8)
- Gizlenecek mesaj verisinin i. pozisyondaki baytın değerini M(i)
- Gizlenecek mesaj verisinin i. pozisyondaki baytın değerinin ilk 4 biti M(i,1:4)
- Gizlenecek mesaj verisinin i. pozisyondaki baytın değerinin son 4 biti M(i,5:8)

Algoritmaya göre ilk olarak oluşabilecek maksimim blok sayısı hesaplanır. Tüm blokları işleme alacak şekilde döngü kurulur. Döngü işlemi sırasında gizlenecek i. pozisyondaki mesaj parçası örtü imgedeki i. pozisyondaki bloğun eşleşme alanları ile sırasıyla karşılaştırılır. Mesaj parçası hangi eşleşme alanıyla eşleşti ise ilgili baytın son biti terslenir. Eğer 1.eşleşme alanı olan EA_1 ile eşleşti ise i.poziyondaki, EA_2 ile eşleşti ise i+1, EA_3 ile eşleşti ise i+2 ve EA_4 ile eşleşti ise i+3.pozisyondaki baytın son biti terslenir. Bu işlem mesajın tüm bitlerinin gizlenmesi veya tüm blokların bitmesiyle sonlanır.

III. BAŞARIM ANALİZİ (PERFORMANCE ANALYSIS)

Şifrelemedeki ana amaç, SMS ile gönderilen bilgilerin Literatürde 4 farklı eşleştirme yöntemine dayalı yöntem ile önerilen yöntemin başarımı kıyaslanmıştır. Buna göre gri tonda bir imgeye 500 baytlık veri gizlenmiş ve değişen bit sayılarını karşılaştırılmıştır.

TABLO I. 500 BAYT GİZLENMİŞ 8 BİTLİK BMP RESMİN VERİ GİZLEME KARŞILAŞTIRMASI [7]

Yöntem	*Değişen Bit Sayısı*	*Gerekli Piksel Sayısı*
İmge Kareleri [8]	1153	18833
Mielikainen [9]	1458	3888
Chan [10]	1285	3888
Hamming matrisi [11]	911	14580
R	1000	25536

Tablo I'e göre önerilen yönteminin Hamming matrisinin performansına çok yakın sonuç üretmiş olduğu gözlenmiş ve diğer üç yönteme göre oldukça başarılı olduğu görülmektedir. Veri gizlemede en az piksel gerektiren Mielikainen ve Chan yöntemleridir. Değişen bit sayıları olarak Hamming, İmge Kareleri ve önerilen yöntem şeklinde başarı sıralaması vardır. Önerilen yöntem daha çok piksele ihtiyaç duymaktadır. Bunun nedeni eşleşme alanı yöntemine göre veri gizleme işlemi yapmasıdır. Bunun yanında imgede en az değişiklik yapmaktadır.

Önerilen yöntemin görsel analizini yapabilmek için 24 bitlik tank imgesine 14.320 bitlik veri hem önerilen yöntemle hemde LSB yöntemi ile gizlenmiştir. Şekil 3'te imgeler görsel görüntüleri verilmiştir. Şekil 3'teki imgeler incelendiğinde önerilen yöntem ile veri gizlenmiş imgenin orjinal imgeden görsel olarak bir farkı yoktur.

a) Önerilen yönteme göre 14.320 bit veri gizlenmiş 24 bitlik tank stego imgesi

b) Orijinal 24 bitlik tank imgesi

Şekil 3. Veri gizlenmiş ve orjinal 24 bitlik tank imgeleri

Bir veri gizleme yönteminin başarısı, steganaliz yöntemlerine karşı dayanıklılığı ile ölçülmektedir. Steganaliz imgedeki değişiklikleri analiz ederek dosya içerisinde gizli verinin varlığını bulmaya çalışır. Gizli verinin tespitinin zor olabilmesi için gizlenecek imgede en az değişiklik yapmak gerekir. Örtü imgesinde ne kadar değişiklik yapıldığını analiz etmek için MSE (ortalama karesel hata) ve PSNR(en yüksek sinyal gürültü oranı) değerleri önem kazanır.

MSE iki imge arasındaki farkı bulmak için geliştirlmiş bir formüldür. Bu formülde iki imgenin piksel değerlerinin farklarının karelerinin toplam piksel değerlerine bölünmesidir. İki imge arasında bir fark yoksa MSE değeri 0'a eşit olur.

$$MSE = \frac{\sum M,N[I_1(m,n)-I_2(m,n)]^2}{M.N} \quad (1)$$

$$PSNR = 10log_{10}\left(\frac{R^2}{MSE}\right) \quad (2)$$

Eşitlik 2'de R imgedeki en büyük piksel değeridir. 8 bitlik gri imge için $R=2^8 -1 = 255$ olur. İki imge birbirinin aynısı ise PSNR sonsuza yaklaşır. Yani

PSNR ne kadar büyükse imgeler arasındaki fark daha azdır.

TABLO II. MSE VE PSNR ANALİZİ

İmge	*Y*	*Z*	*T*	*X*	*MSE*	*PSNR*
Amerika	LSB	22147	88588	2	0,1448	56,523
	R	22147	44294	4	0,0724	59,535
Köpek	LSB	7463	29852	2	0,0997	58,143
	R	7463	14926	4	0,0499	61,145

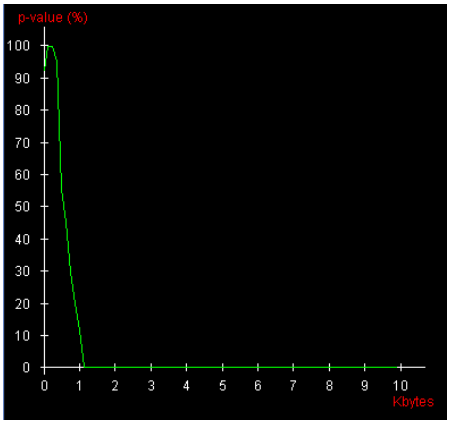
X=Gizlenen/Değişen; Y=Yöntem; Z=Gizlenen very (bayt); T: Değişen Bit

Tablo II'de Amerika ve Köpek isimli imgelere hem LSB hem de önerilen yöntem ile eşit oranda veri gizlenmiştir. Her iki imge içinde önerilen yöntemin başarımı LSB yöntemine gore %100 daha başarılı olduğu görülmektedir. Amerika imgesine 22.147 bayt veri gizlenmiş ve LSB yöntemi ile 88.588 bit değişirken önerilen yöntem 44.294 yarısı kadar bit ile aynı oranda veri gizlemiştir. Önerilen yöntemin MSE değeri LSB yönteminin yarısı kadardır. Buda önerilen yöntemin örtü imgede LSB yönteme göre daha az değişiklik yaptığını göstermektedir. PSNR değerinden de önerilen yöntemin daha başarılı olduğu görülmektedir. Önerilen yöntemin LSB yönteminden en önemli farkı 1 bitlik alana 4 bit veri gizlemesidir. Bundan dolayı imgede daha az değişiklik yapmıştır.

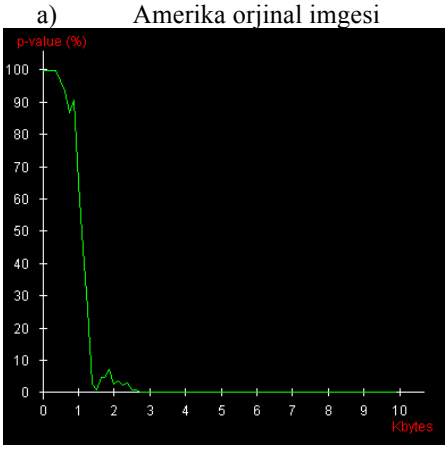
TABLO III. RS STEGANALİZİ

Dosya Gizlenen Veri	*Band Rengi*	*Orijinal*	*LSB*	*Önerilen Yöntem*
Amerika 22.147 Bayt	Kırmızı	1,953%	82,72%	15,71%
	Yeşil	0,211%	0,211%	16,65%
	Mavi	0,414%	0,414%	15,68%
	Toplam	0,860%	27,78%	16,01%
	Gizlenen Boyut (Byte)	657,90	21253,82	12255,16
Köpek 7.463 Bayt	Kırmızı	0,555%	52,08%	6,815%
	Yeşil	0,552%	0,552%	6,623%
	Mavi	0,555%	0,552%	5,988%
	Toplam	0,005%	17,73%	0,064%
	Gizlenen Boyut (Byte)	206,22	6622,22	2418,67

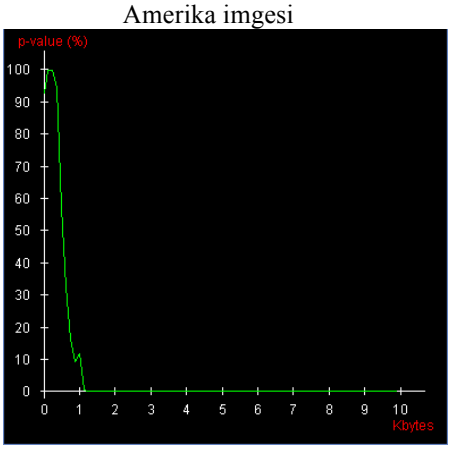
Tablo III'de Amerika ve Köpek imgesinin belirli oranda veri gizlenmiş stego ve orjinal imgeleri için RS steganaliz sonuçları gösterilmiştir. Tablo 3'de verilen Kırmızı, Yeşil ve Mavi alanları RS steganaliz kanal olasılıklarını, Toplam alanı toplam olasılığı göstermektedir. Gizlene Boyut alanı ise imgelere gizlenen verilerin boyutu için RS analiz tahminini göstermektedir. Analiz sonuçları incelendiğinde RS yönteminin verdiği sonuçlara göre önerilen yöntemin imgede daha az değişiklik yaptığı ve LSB yöntemine göre yarı yarıya daha düşük değerler verdiği gözlenmiştir. 24-bitlik Amerika imgesine hem LSB ile hem de önerilen yöntem ile 22.147 bayt veri gizlenmiştir. Şekil 3'de her iki yöntemle oluşan stego imgelerin ki-kare sonuçları verilmiştir.



a) Amerika orjinal imgesi



b) 22.147 bayt LSB yöntemi ile veri gizlenmiş Amerika imgesi



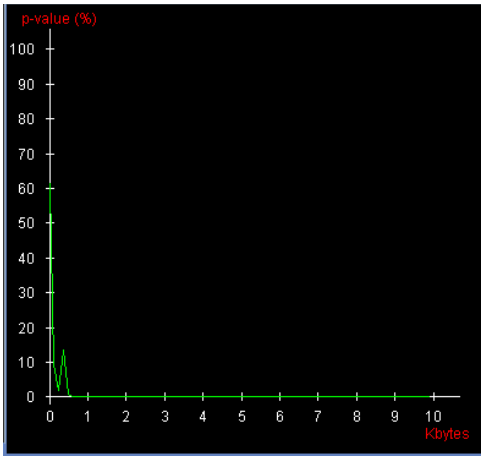
c) 22.147 bayt önerilen yöntem ile veri gizlenmiş Amerika imgesi

Şekil 4. Ki-kare steganaliz sonuçları

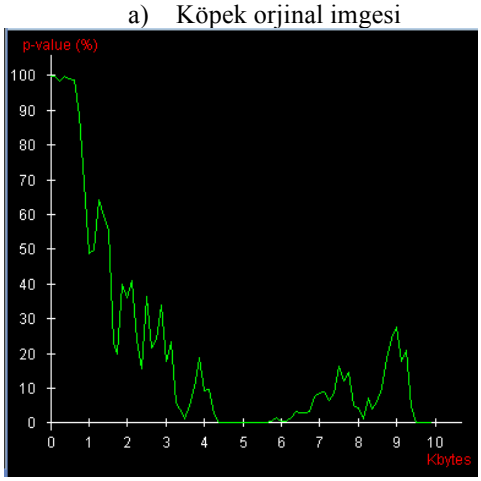
Şekil 4'te kikare steganaliz sonuçları incelendiğinde LSB yöntemine göre önerilen yöntemin sonuçları orjinal imgenin ki-kare sonuçlarına çok yakın çıkmıştır. Buda önerilen yöntemin imgede çok daha az değişiklik yaptığını göstermektedir. Ki-kare yöntemi, önerilen yöntem ile gizlenen verileri tespit edememiştir.

24-bitlik Köpek imgesine hem LSB ile hem de önerilen yöntem ile 7.463 bayt veri gizlenmiştir. Şekil

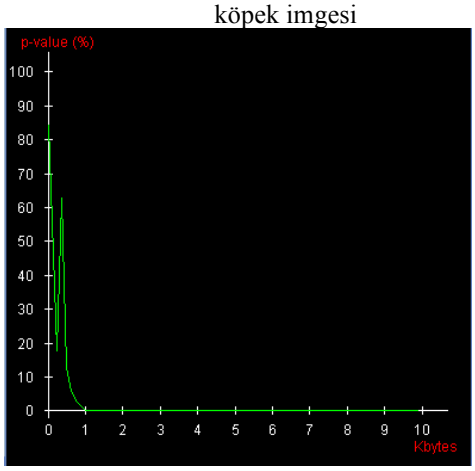
4'de her iki yöntemle oluşan stego imgelerin ki-kare sonuçları verilmiştir.



a) Köpek orjinal imgesi



c) 7.463 bayt LSB yöntemi ile veri gizlenmiş köpek imgesi



c) 7463 bayt önerilen yöntem ile veri gizlenmiş köpek imgesi

Şekil 5. Ki-kare steganaliz sonuçları

Şekil 5'te ki-kare steganaliz sonuçlarına göre LSB yöntemine göre önerilen yöntemin sonuçları orjinal imgenin sonuçlarına çok yakın çıkmıştır. Buda önerilen yöntemin örtü imge de çok daha az değişiklik yaptığını göstermektedir. Ayrıca ki-kare yöntemi önerilen yöntem ile gizlenen verileri tespit edememiştir.

IV. SONUÇ (CONCLUSION)

Bu makalede sunulan çalışmanın amacı, bilgi iletişiminin güvenli olmadığı internet gibi ortamlarda güvenli iletişim için uygulanan sırörtme yöntemlerini anlatmak ve yeni bir sırörtme yöntemini sunmaktır. Önerilen yöntem geleneksel LSB yöntemine göre örtü imgede %100 oranında daha az değişiklik yapmaktadır. Ayrıca Hamming, Chan, Mielikainen ve imge kareleri yöntemlerine göre örtü imgede daha az değişiklik yaptığı gösterilmiştir. Ki-kare ve RS steganaliz sonuçlarına göre de önerilen yöntemin saldırılara karşı dayanıklı olduğu gösterilmiştir.

V. KAYNAKLAR (REFERENCES)

[1]. M. Kalenderi, D. Pnevmatikatos, I. Papaefstathiou, C. Manifavas, "Breaking The Gsm A5/1 Cryptography Algorithm With Rainbow Tables And High-End Fpgas", 2010

[2]. The World in 2010-The rise of 3G, [Offline]. Available: http://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf, 2010

[3]. Smartphone OS Market Share, IDC [Online]. Available: http://www.idc.com/prodserv/smartphone-os-market-share.jsp, 2015

[4]. J. F. DiMarzio, Androıd A Programmers Guıde, McGraw Hill Professional, 2008

[5]. P. Haghirian, M. Madlberger, A. Tanuskova, "Increasing advertising value of mobile marketing – An empirical study of antecedents", Presented at 38th Hawaii International Conference on System Sciences, 2005.

[6]. N. Faruk, A.A Ayeni, M. Y. Muhammad, L.A. Olawoyin, A. Abdulkarim, J. Agbakoba, M. O. Olufemi, "Techniques for Minimizing Power Consumption of Base Transceiver Station in Mobile Cellular Systems", International Journal of Sustainability, VOL.2 No.1, 2013

[7]. Digital cellular telecommunications system (Phase 2+); Circuit switched voice capacity evolution for GSM/EDGE Radio Access Network (GERAN) (3GPP TR 45.914 version 11.0.0 Release 11) ETSI TR 145 914 V11.0.0 (2012-11) ETSI. 2012

[8]. Y. L. Ng, "Short Message Service (SMS) Security Solution for Mobile Devices", Naval Postgraduate School, 2006

[9]. R. R. Chavan, M. Sabness, "Secured mobile messaging" in International Conference On Computing, 2012.

[10]. A. Lecturer, "A Symmetric Key Cryptographic Algorithm", Hindu College of Engineering, 2010

[11]. P. Pimpale, R. Rayarikar, S. Upadhyay, "Modifications to AES Algorithm for Complex Encryption", IJCSNS International Journal of Computer Science and Network Security, Vol.11 No.10, 2011.