افزایش امنیت داده‌ها در سیستم‌های اطلاعات مکانی

صدیقه ابراهیمی‌فر
شرکت آب و فاضلاب استان کرمان
امیر صحراکار
شرکت آب و فاضلاب استان کرمان

چکیده
سیستم اطلاعات جغرافیایی (GIS) نقش حیاتی در بسیاری از کاربردها از جمله در صنعت آب و برق ایفا می‌کند که کاربرد موفقیت‌آمیز در این حوزه نیازمند دقت، صحت و محرمانگی اطلاعات است. در عصر ارتباطات دیجیتال، GIS نقش مهم و کلیدی در تصمیم‌گیری و ارائه برنامه‌های استراتژیک در تمام حوزه‌ها در صنعت آب و برق دارد. از دست رفتن صحت و محرمانگی داده‌ها و تصمیمات اشتباه در صنعت پیامدهای سنگینی در یک ناحیه ایجاد می‌کند و یک حمله بیوتروریسمی را رقم می‌زند و این موضوع حساس بودن اطلاعات آب و برق و حفظ امنیت اطلاعات را در این حوزه بیش از پیش نشان می‌دهد. در سیستم پیشنهادی ارائه شده، ما مکانیزم ترکیبی پنهان نگاری و رمزگذاری برای محافظت از داده‌های GIS را معرفی کرده‌ایم که با ارسال اطلاعات از طریق تصویر و رمزگذاری ترکیبی راهکاری برای حفظ امنیت داده‌ها بیش از گذشته ارائه داده‌ایم.

واژگان کلیدی: GIS، رمزگذاری، امنیت، داده‌های اطلاعات مکانی

مقدمه

امروزه استفاده از سیستم‌های اطلاعات مکانی، GIS، در کاربردهای بسیاری از جمله کاربردهای تجاری، نظامی، دولتی و ... اهمیت زیادی پیدا کرده است و نقش موثری در تصمیم‌گیری‌های مدیران و تصمیم‌گیری‌های هوشمند و جلوگیری از حملات بیوتروریسم ایفا می‌کند، از این رو صحت، دقت و محرمانگی اطلاعات مکانی اهمیت ویژه‌ای دارد که مسلتزم امنیت داده‌ها می‌باشد. در این مقاله بر آن شدیم به راهکاری برای حفظ امنیت اطلاعات داده‌های مکانی بپردازیم. در راهکار ارائه شده از روش ترکیبی پنهان نگاری و رمزگذاری استفاده می‌کنیم.

تحقیق به این صورت ادامه پیدا می‌کند که در بخش‌های بعدی به کارهای مرتبطی که تا کنون ارائه شده‌اند می‌پردازیم سپس راهکار پیشنهادی را ارائه می‌دهیم، و راهکار ارائه شده را مورد بررسی و ارزیابی قرار می‌دهیم و در آخرین بخش نتایج را بیان می‌کنیم.

رمزگذاری و پنهان نگاری

رمزگذاری و پنهان نگاری و بسیاری از فناوری‌های دیگر برای مقابله با تهدیدات امنیتی مورد استفاده قرار می‌گیرند که هر کدام از این روش‌ها محدودیت‌ها، کاربردها و اهداف خود را دارند.

رمزگذاری سعی می‌کند از اطلاعاتی که در حال انتقال در شبکه هستند محافظت کند به گونه‌ای که سه اصل محرمانگی، اصالت و یکپارچگی در آن‌ها حفظ شود. در رمزگذاری، داده‌ها قبل از ارسال در سمت فرستنده با استفاده از کلید و الگوریتم رمز شده و بعد از انتقال و دریافت در سمت گیرنده، با عملیاتی معکوس، داده‌ها رمزگشایی می‌شوند. بسیاری از الگوریتم‌های متقارن و نامتقارن مانند ASE, RSA, Hashing و موارد دیگر برای این منظور استفاده می‌شوند. کارایی رمزگذاری به مدیریت کلید و توزیع آن بستگی دارد. رمزگذاری اطلاعات را به صورت غیرقابل فهم در می‌آورد که بدون کلید قادر به رمزگشایی نمی‌باشد.

پنهان نگاری اطلاعات روشی است که می‌توان اطلاعات موردنظر را در قالب یک عامل پوشاننده با بیشترین میزان دقت به امنیت، بین نقاط مورد نظر جابجا کرد به صورتی که حتی اگر در طی مسیر اطلاعات از طریق افراد غیرمجاز مورد دسترسی قرار گرفت امکان دستیابی به داده‌های پنهان شده وجود نداشته باشد. در واقع پنهان نگاری هنر و علم جاسازی اطلاعات در یک رسانه میزبان مانند متن، صدا، تصویر و غیره است. در پنهان نگاری هدف اصلی، امنیت به معنای عدم توانایی در اثبات وجود پیغام است (Almuhammadi and Al-Shaaby, 2017).

با ترکیب دو روش رمزگذاری و پنهان نگاری می‌توان سطح بالایی از امنیت را برای انتقال داده‌های اطلاعات مکانی فراهم نمود.

کارهای مرتبط

طی سال‌های گذشته سیستم‌های GIS بسیار پرکاربرد شده‌اند و مورد توجه دولت‌ها برای انتقال اطلاعات قرار گرفته‌اند. پژوهش‌های بسیاری در زمینه کاربردهای GIS تا کنون انجام شده است و کمتر به نقش امنیت در انتقال داده‌های حساس اطلاعات مکانی اهمیت داده شده است. مرجع (Kiedrowicz, 2019) به ارائه یک معماری جهت تضمین امنیت داده‌ها در پایگاه داده اطلاعات مکانی پرداخته است. پژوهش‌های بسیاری در زمینه حفظ اطلاعات محرمانه با استفاده از رمزگذاری و پنهان نگاری به صورت روش‌های جداگانه و روش ترکیبی صورت گرفته است. مرجع (Alvi and Dawes, 2013) با استفاده از منطق فازی و تکنیک‌های پردازش تصویر برای توسعه، یک طرح پنهان نگاری تصویر غیر قابل مشاهده ارائه کرده است. در مرجع (Aswathy and Job, 2014) یک طرح ترکیبی از رمزگذاری و پنهان‌نگاری برای دسترسی به اطلاعات ارائه شده است که سطح امنیت را افزایش می‌دهد. این روش دو مرحله امنیت را پیشنهاد می‌کند: اولی فرآیند رمزگذاری ودومی افزایش سطح امنیت پنهان نگاری برای مخفی کردن اطلاعات است. در مرحله اول پیام ارسال شده و به یک تصویر رمز با استفاده از فرایند اول رمزگذاری تبدیل شده است. سپس در مرحله دوم این تصویر رمز به یک

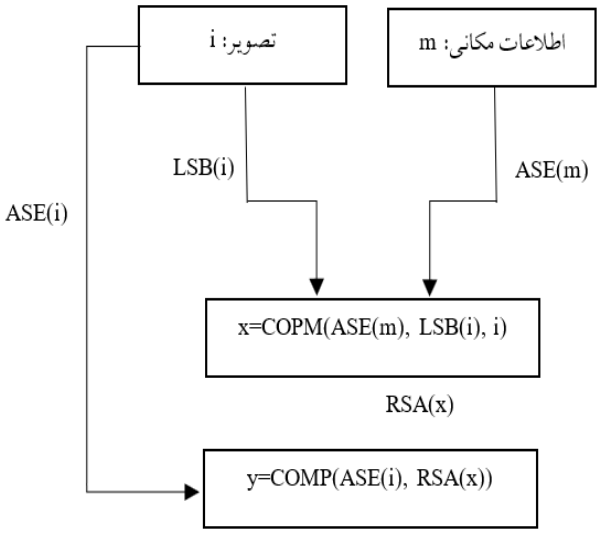
متن میانی با استفاده از دومین فرآیند رمزگذاری تبدیل شده است. متن رمز میانی یا اطلاعات در داخل یک تصویر پوشش با استفاده از فرآیند پنهان نگاری درج می‌شود. مرجع (Sajasi and Moghadam, 2015) یک طرح غیر قابل برگشت برای پنهان کردن تصویر ارائه داده است که قادر به بهبود کیفیت بصری و امنیت تصویر پنهان نگاری شده می‌شود. این کار توسط یک طرح پنهان نگاری ترکیبی شامل تابع میدان دید نویز (NVF) و و آشوب بهینه مبتنی بر طرح رمزگذاری بدست آمده است.

روش پیشنهادی

در این بخش به ارائه مدلی با هدف حفظ بیشتر امنیت اطلاعات مکانی می‌پردازیم. در روش پیشنهادی از پنهان نگاری داده‌ها همراه با رمزگذاری AES در سطح اول استفاده می‌کنیم و در سطح دوم ترکیب اطلاعات رمز شده و پنهان‌نگاری انجام می‌شود و در سطح سوم خروجی سطح دوم را با الگوریتم RSA و تصویر را با ASE رمز کرده و با هم ترکیب می‌کنیم. برای پنهان نگاری روش LSB را انتخاب کرده‌ایم.

رمزگذاری سمت فرستنده

مدل پیشنهادی و ترتیب مراحل (شکل ۱) سمت فرستنده به شرح زیر می‌باشد.



شکل ۱- رمزگذاری سمت فرستنده

ورودی‌ها:

m: اطلاعات مکانی که باید در شبکه انتقال یابد.

i: تصویر انتخاب شده جهت پنهان کردن اطلاعات مکانی

مرحله ۱:

۱. با استفاده از الگوریتم رمزگذاری AES-128bit، m را رمزگذاری کرده و ASE(m) بدست می‌آید.

۲. کم ارزشترین بیت‌های پیکسل‌های تصویر i را استخراج کرده و LSB(i) بدست می‌آید.

مرحله ۲: ASE(m) و LSB(i) را در تصویر i ترکیب کرده و در سطح اول، اطلاعات رمز شده و پنهان شده x بدست می‌آید:

x=COPM(ASE(m), LSB(i), i)

مرحله ۳:

۱. با استفاده از الگوریتم RSA، x را رمزگذاری می‌کنیم و RSA(x) بدست می‌آید.

۲. تصویر i را با استفاده از الگوریتم ASE رمزگذاری کرده و ASE(i) بدست می‌آید.

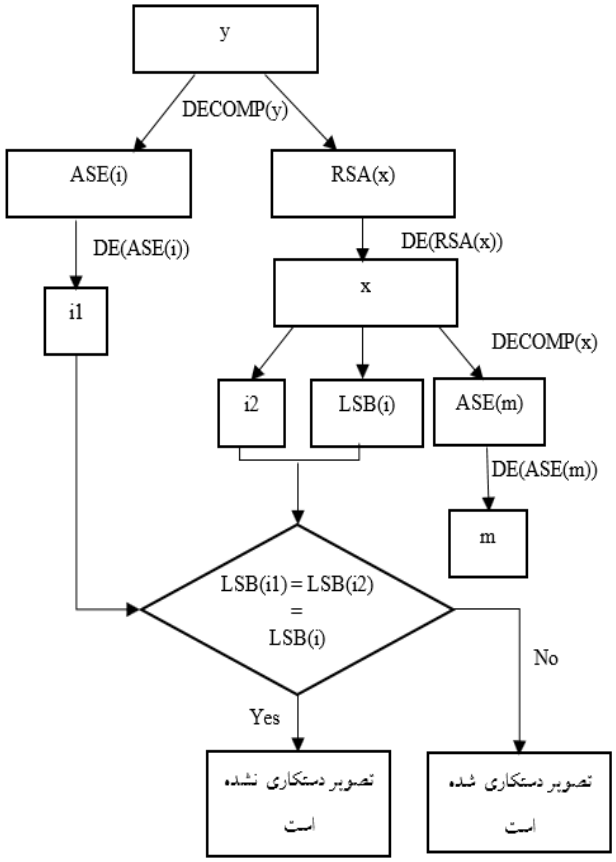
مرحله ۴: RSA(x) و ASE(i) را ترکیب کرده و پیام رمزگذاری نهایی y بدست می‌آید.

y=COMP(ASE(i), RSA(x))

اطلاعات مکانی رمزگذاری شده و پنهانگاری شده y، آماده ارسال از سمت فرستنده می‌باشند.

رمزگشایی سمت گیرنده

اطلاعات رمز شده پس از دریافت در سمت گیرنده باید رمزگشایی و خوانا شوند. رمزگشایی اطلاعات مکانی در چهار سطح انجام می‌پذیرد. در سطح اول تجزیه پیام دریافت شده، انجام می‌شود. در سطح دوم دیکد کردن پیام و تصویر و در سطح سوم مجدد تجزیه پیام انجام می‌شود و درسطح آخر صحت و امنیت اطلاعات مکانی بررسی می‌شود. ترتیب مراحل رمزگشایی به شرح زیر می‌باشد:



شکل ۲- رمزگشایی سمت گیرنده

ورودی:

y: پیام رمزشده دریافت شده از ارتباطات ناامن

مرحله ۱: y با استفاده از تابع DECOMP(y) به RSA(x) و ASE(i) تجزیه می‌شود.

مرحله ۲: به صورت همزمان

۱. با استفاده از الگوریتم دیکد RSA، x استخراج می‌شود.

x=DE(RSA(x))

۲. با استفاده از الگوریتم دیکد ASE، تصویر i1 استخراج می‌شود.

i1=DE(ASE(i))

مرحله ۳: x با استفاده از تابع DECOMP(x) به ASE(m)، LSB(i) و i2 تجزیه می‌شود.

مرحله ۴: اطلاعات مکانی m، با استفاده از الگوریتم دیکد ASE از ASE(m) بدست می‌آید.

مرحله ۵: LSB(i1) و LSB(i2) محاسبه شده و با LSB(i) مقایسه می‌شوند. اگر هر سه برابر باشند یعنی تصویر دستکاری نشده و نشان‌دهنده حفظ امنیت اطلاعات مکانی m است.

if LSB(i)=LSB(i1)=LSB(i2)

then

“True”

ELSE

“False”

بررسی روش پیشنهادی

در روش ارائه شده در چند سطح از روش رمزگذاری استفاده شده است. استفاده از الگوریتم‌های متقارن ASE و نامتقارن RSA برای رمزگذاری امنیت سیستم را افزایش می‌دهد.

از طرف دیگر استفاده از پنهان‌نگاری و ترکیب اطلاعات رمزشده با پنهان نگاری LSB نیز باعث افزایش امنیت سیستم خواهد شد.

ایجاد کپی‌های رمزگشایی شده از یک تصویر در سمت گیرنده و مقایسه آنها به سادگی بررسی صحت اطلاعات مکانی کمک کرده و امکان تشخیص درست بودن اطلاعات را ساده ساخته است.

الگوریتم نامتقارن RSA سرعت پایین‌تری نسبت به الگوریتم ASE دارد اما به توجه به ایجاد سطح امنیت بیشتر توسط این الگوریتم، تنها یکبار استفاده از آن در رمز کردن اطلاعات حساس منطقی می‌باشد.

نتیجه‌گیری

در این مقاله، مدلی برای ارسال داده‌های اطلاعات مکانی حساس در بستر شبکه ارائه دادیم که با توجه به چندین مرحله رمزگذاری و ترکیب با پنهان نگاری، سطح امنیت را افزایش می‌دهد. اگر به هر ترتیبی یک نفوذگر بتواند در یک مرحله پیام را رمزگشایی کند در سایر مراحل با سختی روبرو خواهد شد. همچنین استفاده از هر دو شیوه رمزگذاری متقارن و نامتقارن نیز بر سطح امنیت سیستم بیش از پیش می‌افزاید.

مدل ارائه شده سطح امنیت بسیار خوبی را برای اطلاعات مکانی حساس فراهم می‌آورد. در تحقیقات آینده می‌توان به بررسی و افزایش سرعت اجرای این الگوریتم پرداخت.

منابع

S. Almuhammadi and A. Al-Shaaby, (2017). “A survey on recent approaches combining cryptography and steganography,” Computer Science & Information Technology (CS & IT).

[M. Kiedrowicz, (2019). “Methodology of ensuring the security of gis spatial data,” 26th Geographic Information Systems Conference and Exhibition (gis odyssey 2019), pp.97-108.

A.K. Alvi, and R. Dawes, (2013). “Image steganography using fuzzy domain transformation and pixel classifications,” In proceeding of: The 25th International Conference on Software Engineering and Knowledge Engineering (SEKE2013), pp. 192-195.

A. Aswathy Nair and D. Job, (2014). “A secure dual encryption scheme combined with steganography,” IJETT-Volume 13 Number 5, PP. 218-225, 2014.

S. Sajasi, A. Moghadam, (2015). “An adaptive image steganographic scheme based on noise visibility function and an optimal chaotic based encryption method,” Elsevier, Applied Soft Computing 30, PP. 375–389, 2015.

Increasing Security Data in GIS

Sedighe Ebrahimifar

Water and Sewerage Company

Amir Sahrakar

Water and Sewerage Company

1-1-

1-2- Abstract

Geographic information system (GIS) plays a vital role in many applications, including in the water and electricity industry, where successful application in this field requires accuracy and confidentiality of information. In the era of digital communication, GIS plays an important and key role in making decisions and providing strategic plans in all areas in the water and electricity industry. The loss of data integrity and confidentiality and wrong decisions in the industry create heavy consequences in an area and constitute a bioterrorist attack, and this issue shows the sensitivity of water and electricity information and maintaining information security in this area more than ever. In the proposed system, we have introduced a hybrid mechanism of encryption and encryption to protect GIS data. By sending information through image and hybrid encryption, we have provided a solution to keep data more secure than before.

1-3- Keywords GIS, encryption, security, geospatial data.